

Bitcoin Exposed

Today's Complete Guide
to Tomorrow's Currency



Daniel Forrester & Mark Solomon

Bitcoin Exposed:

Today's Complete Guide to Tomorrow's Currency

Learn the Ins and Outs of Bitcoin and How You Can Profit From It

By Daniel Forrester
&
Mark Solomon

Editor's Foreword

We are all accustomed to our currencies, whether they are dollars, euros, yen, yuan, or reals.

However, We Rarely Stop To Ask:

- Who controls the currency we depend on?
- Can “they” make my currency worthless?
- Do the people or institutions that control the currency we use have an advantage over us? Does this advantage allow them to live more easily, become richer and not have to work like we do for the currency? (Hint: YES!)

There’s a new currency in town, one that is beginning to change how the world’s nations, marketplaces, and peoples interact financially.

What To Expect From This Book:

- Learn all the basics of Bitcoin, from how to buy them, use them, sell them, and even create (mine) them.
- Discover the top 8 dangers for Bitcoin users.
- A step-by-step guide to creating one’s own Bitcoins, with only the computer you have now. Plus learn how to become a super Bitcoin creator (miner).
- An essential, informative chapter, “How to Trade Bitcoins”. While not guaranteeing anyone profits, these techniques have produced consistent and large trading profits across several markets over thousands of trades.
- How to avoid the many, advanced Bitcoins scams on the Internet. There are ways to avoid them and this guide shows you how.
- Learn the right way and many wrong ways to set-up Bitcoin use. You’ll learn how to steer clear of common mistakes, and how to safely venture into the Bitcoin world.

Table Of Contents

Why Are Bitcoins The Secret To A Better World, True Freedom And A Rich Retirement?

How To Use This Book

Fundamentals: Overview of Bitcoin

- What Is A Bitcoin
- Where Did Bitcoin Come From And Why Does It Matter?
- Why Should I Buy Or Use Bitcoins?
- What Are Bitcoins Really Worth?

History Of Digital Currencies – And How They Lead To Bitcoin

- Digital Gold, Silver, False Promises And Digital Scams
- Who Hates Bitcoin And Why?
- Why Bitcoin Is Different And Better Than Everything – Almost.

How To Use Bitcoins

- Getting Your First Bitcoin
- Spending Bitcoins
- Saving Bitcoins
- Investing In Bitcoins, Or Not
- Protecting Bitcoins
- Transferring Bitcoins
- Accepting Bitcoins In Business
- Using Bitcoins Anonymously

How To Create Bitcoins Or Become A Bitcoin Miner

- The Concept Of Bitcoin Mining
- How To Mine Bitcoins
- Problems In Mining Bitcoins

Potential Bitcoin Disasters, Problems, And Challenges

- Failure Analysis Of The Bitcoin System
- Main Targets For Hacks And Attacks
- Prominent Attacks, Scammers, And Bottlenecks

Profiting With Bitcoins

- Trading Bitcoins
- General Trading Principles For Bitcoin
- Bitcoin Application Development

Future Of Bitcoin And Alternative Currencies

- Opportunities And Dangers Ahead
- Agents For And Against Bitcoin; Alternative Currencies
- Predicting Prices For Bitcoins
- Expansion Markets For Bitcoins

- **One Last Thing**

Appendices

Appendix A – Major Bitcoin Developments & Timeline

Appendix B – List of main Bitcoin Services and Web sites

Appendix C – Bitcoin Terminology

Appendix D – Bitcoins Mathematical Basis

Why Are Bitcoins The Secret To A Better World, True Freedom And A Rich Retirement?

“All great ideas are dangerous.”

Oscar Wilde

Bitcoin is the bridge to a new, vastly freer, dependable, honest, and democratic world. Of course we can simply use Bitcoins for fun, profit, and online transactions if that is all we are after.

Why stop there though? When using Bitcoins, we enter a system with massive benefits which include: almost no fees for transfers such as bank wires, the possibility of complete anonymity or privacy with all the financial privileges, and no central bankers or government stealing your Bitcoins. Bank account theft has recently occurred in the banks of Cyprus, as well as in Argentina. This, in addition to worldwide inflation, has encouraged people to look for a better banking solution.

Bitcoin takes the reins from those people, institutions, and even governments that control our currencies, and puts the control levers solely in all of our hands. Yes, we finally get to control our own currency.

Bitcoins can unlock the guarded door of prosperity by raising the wealth and prosperity of everyone. It helps accomplish this by being a *deflationary* currency. Bitcoins increase in value relative to dollars or euros, etc. by default because of the limited amount of Bitcoin currency entering the system. This helps make the same amount of Bitcoins buy *more* stuff we need year after year.

Bitcoin can free us from the prying eyes of tax codes, bank fees, or any number of confiscation games played by governments, banks, and “authorities.” While this is a controversial application of Bitcoin, this book would be incomplete without explaining the privacy opportunities Bitcoin offers.

For example, if we send money from our traditional bank account to an acquaintance of ours using another bank account in a different country, the following rules and fees may apply:

1. We may not be allowed to send the money. Any country the U.S. bans from trade, including (at one time or another) - Cuba, Sudan, North Korea, Iran, Belarus, Syria, Burma, Zimbabwe, etc. (And tomorrow, who knows..)
2. Fees will often be \$25-\$50+ outbound, and possibly \$25+ inbound.
3. Banks can block the wire, or return the money within 48 hours. Also, the receiver may even pull more money out of our account depending on the transfer rules.
4. Banks often convert foreign currencies at a discount, taking additional profit off the top of our transfer.
5. Both parties are now known to the bank and the government for better or for worse.
6. The government can decide to tax funds being transferred outside the country. This can be as high as 30% for foreign banks that do not adhere to U.S. bank rules. That hurts!
7. Not only are the banks taking huge fees for the transfer of our money, but they can take as long as 24 hours or even more in some cases. We are paying Ferrari prices, and getting moped performance.

This gives you a small sample of the financial pain involved with using standard currency, the U.S. dollar, and standard banks.

The same transaction using Bitcoins would involve the following:

1. No bank fees.

2. No foreign currency buy/sell fees.
3. A small \$0.25, (yes, you read that correctly - one quarter) service fee from a site such as dwolla.com
4. No one needs to know whom the buyer or seller is. Complete privacy for all parties.
5. Any country, any person, and any transaction at any time is completely allowed.
6. There will be tax implications depending on your reporting, not on a bank reporting on you.
7. Best of all, our Bitcoin transfer will occur nearly instantly. The minute we press SEND, the recipient can access his or her new stash of Bitcoins, and continue his cigar factory tour of Cuba, with no one the wiser. Hope he brings back some Bolivars for our generosity!
8. They can then transfer the Bitcoins from his Bitcoin wallet through an in/out exchange such as mtgox.com or other exchange into his foreign bank account.

Bitcoin has so many advantages, with only a few key disadvantages, that it deserves all the attention it is receiving. This guide will help any reader understand how to join the wave of those converting to Bitcoin. Offering great potential for inexpensive money transfers, convenient shopping, secure wealth preservation, and ultimately, freedom, Bitcoin may end up being the story of the century.

How To Use This Book

“If you hold a cat by the tail, you learn lessons you cannot learn any other way.”

Mark Twain

Novice Bitcoin users, or those who have never even heard of Bitcoin, will be best served going through most of the chapters in order, with the possible exception of How to Mine for Bitcoins. That section may not offer any value if all one wants is to use Bitcoins. After completely reading this guide, any Bitcoin conversation - save for the most mathematically involved ones, will sound familiar and be easily understood.

If you have bought a few Bitcoins, transacted some with them, but still have questions about the future, the various opportunities with Bitcoin as well as the risks, then the only chapter to skip is the one discussing [How to Use Bitcoins](#). Still, there are probably a lot of Bitcoin users that could benefit from tips, techniques, and security steps that they are not using and might want to.

For the experienced Bitcoin user, the most useful sections will probably be about trading Bitcoins profitably ([Profiting with Bitcoins](#)), and predictions for the future of Bitcoin ([Future of Bitcoin and Alternative Currencies](#)). Though this is not a complete trading guide by any stretch, even an experienced Bitcoin user can learn some of the science and art leading to more consistent profits through buying and selling Bitcoins. Also, the future of Bitcoin - admittedly challenging to predict - offers the best trade opportunity of all. Either go long with everything we have, or short it to the floor. Both could bring huge returns, depending on time. Trading skills will bring these questions and their answers into much clearer focus.

Being the fastest growing financial phenomenon in the world means there will be changes by the minute.

Stay on top of the Bitcoin changes by signing up with:

www.publisherswebsite.com

And also with:

www.financialsurvivalcenter.com

Applying the same trading analysis that spotted the gold and silver bull and bear market, the dot-com bubble, real estate bubbles, along with biotech opportunities, Bitcoin trading advice and trend predictions are now part of the Financial Survival Center wealth preservation and profit producing system.

Fundamentals: Overview Of Bitcoin

“So you think money is the root of all evil? Have you ever asked what is the root of all money?”

Ayn Rand

Bitcoin is simply the name given to the new digital, internet-based form of currency. While going beneath the surface of the basic concept of a Bitcoin gets somewhat complicated, knowing the mathematics behind the creation of Bitcoin and its operations, are not necessary. We can use, profit with, and generally understand what Bitcoin is, and why Bitcoin is important in our everyday lives, while the genius behind it hums along in the background.

Best of all, our journey into the Bitcoin world brings benefits from all corners. Financially, we can spend less on transactions with Bitcoins while seeing our ability to buy products increase with the increase in Bitcoin's value. Value increases are not guaranteed of course. And our privacy will become almost impenetrable if we choose that route.

We can create an online business accepting Bitcoins with almost no hassle (such as fees and complications we would encounter trying to accept credit cards). Even dealing with the minor annoyance of learning new terms and concepts seems like a small price to pay for the mother lode of benefits Bitcoin delivers. Far off but critically important is the future treasure Bitcoin promises to deliver. Those future benefits will be covered in the last chapter because they are potentially earth shattering in scope, and there is much ground to be covered before we get there.

Bitcoin's story reads something like a Tom Clancy novel. There are secret agents. Trusted double agents try to sell out the cause. Murders happen, or something close to it. Prison time for innocent men. Fortunes made by criminals. Bigger fortunes lost by the risk takers. Geniuses, madmen, Libertarians, Socialists, government forces, and Anarchist hackers all working together, before fighting each other tooth and nail. (Okay, even I'll admit this is a *bit* of an exaggeration, but you get the point!).

We would expect nothing less considering Bitcoin is battling the most powerful forces on earth. Based on the rapid growth from \$0.06 to over \$200 (and back down to around \$100), Bitcoin is winning the battle.

David versus Goliath is playing before our very eyes with the same result expected. The little guys (us) are taking on the powers that control the money universe and government (PTB - powers that be), and knocking them for a loop. Welcome to the new, exciting world of Bitcoin. You will be absolutely glad you came.

What Is A Bitcoin?

Bitcoin is largely an imaginary piece of code, with no intrinsic value. Gold has intrinsic value for use as jewelry, some in electronics, for making teeth, for coating mirrors, and a host of other possibilities. Silver has even more intrinsic value for medical uses, in film, in coatings for bearings, for its heat distribution and electrical properties, etc. Bitcoins, gold, and silver all share one crucial aspect in common. They are all relatively rare.

Bitcoins are like the rewards for a correct answer to a certain math problem. Both the problem and the answer are completely unique. There will be a limit of about 21 million (the eventual exact number is 20999999.97690000) of these special solution rewards known as the “Bitcoin.”

Those dabbling in the complicated technicalities of Bitcoin, such as programmers and promoters, call it a “crypto-currency.” This invented term refers to the form of mathematics that generates the rarity behind the solutions that earn the Bitcoin rewards.

Nuts and bolts for Bitcoin look like this:

Bitcoin is often represented as BTC, or 1 BTC is 1 Bitcoin.

We can also deal with 0.1 BTC, 0.01 BTC as we would with say, U.S. dollars. \$0.01 USD is also known as 1 cent. Similar for Bitcoins though, it has software behind it that allows for a very small denomination of a Bitcoin that looks a tad scary:

0.00000001 BTC.

or 100 millionth of a Bitcoin

This smallest unit of BTC is known affectionately as a “Satoshi” in honor of the genius that developed the whole code framework. Not that the use is popular, but we use the same names from the metric system when describing Bitcoin denominations:

CentiBitcoin is also a bitcent and looks like .01 BTC or 1 cBTC

MilliBitcoin is either a bitmil or mbit: .001 BTC or 1mBTC

That is about all we will need for the foreseeable future. For the purists though, the smallest, fashionable BTC is the microbit or ubit with .000001 BTC or 1 uBTC.

If we find ourselves trading in uBTC's soon then let's hope we all stocked up on BTC's before the attack of the 5 zeros!

Bitcoins In Use

We can now buy things with Bitcoins. No cars, planes, diamonds, or furry dinosaur feet are available yet with Bitcoins because it is too new, not fully understood, and somewhat risky. However, many retailers are coming around to Bitcoin; here is what a Bitcoin shopping payment looks like from a website called BitcoinIn:



Notice how the prices already use .001 BTC format. The reason is, Bitcoins exploded in value compared to other currencies. We value Bitcoins in our national currencies. If we live in the U.S., our national currency is the U.S. dollar or USD for short. Europeans, for the most part, use euros or €.

Out of the gates, Bitcoin was a 6-cent weakling with 1 BTC being priced at 0.06 USD. So the same items we now see priced at 0.294BTC would have been around .416 BTC in Bitcoin's toddler days of 2009-2010. Now that Bitcoin is a fast growing online option for payments, we can expect to see it continue to go deeper into the bitcent, mbit and even ubit prices.

Keep this impressive example in mind for a later section explaining why Bitcoin is one of the secrets to personal and financial freedom.

Where Did Bitcoin Come From And Why does it Matter?

Officially, Bitcoin started in 2009 by a mystery man (or group) with the Japanese name of Satoshi Nakamoto. His name has the same commonality as John Smith has in the U.S. In short, we do not know who started Bitcoin. He kept his identity secret for an important reason.

The domain name, Bitcoin.org was created in 2008 in Helsinki from whois.org. One common theory is that three programmers skilled in cryptography - none of them Japanese - developed the system. The men behind one of the relevant patents #20100042841 are Neal King, Vladimir Oksman, and Charles Bry. All three have filed several related patents in the encryption, and network management area.

A fantastic article making a strong case for the three man origin of Bitcoin appeared on Fastcompany.com (<http://www.fastcompany.com/1785445/Bitcoin-crypto-currency-mystery-reopened>)

Unsurprisingly, all three potential inventors strongly deny they are involved at all.

The Atlantic Wire has tagged a British coder named Michael Clear as the brain behind Bitcoin. He too denies it. (<http://www.theatlanticwire.com/technology/2011/10/race-unmask-Bitcoins-inventors/43535/>)

With nobody pinned as the founder of Bitcoin, this anonymity becomes one of its great strengths. There is no founder to throw in jail. There is no central Bitcoin bank to shut down. There is no one man, woman, or group controlling Bitcoin.

Bitcoins come from a distributed network of people running what are called Bitcoin miners. We will be discussing Bitcoin mining later on in this book. Having a central processing or controlling location for a currency presents a big problem. Governments, hackers, banks, or general criminals can all attack and often destroy that central authority.

Governments go after alternative currencies. A successful precious metal backed electronic currency called e-gold stirred the ire of government. The founder and head, Dr. Douglas Jackson, was nearly sent to prison for 20+ years.

Several ideas for currencies similar to Bitcoin have come and gone. Around 1994, Digicash was an early attempt at a central, online, digital currency using code-breaking math. Peppercoin was another code-based version of digital currency a bit later, but it also failed.

What these early attempts lacked was a way of spreading out the ability to generate the currency. As in the real world, we could all choose to go search for gold or silver. Some of us may even find a bit of precious metals. A few of us, very few, will find a mother lode. That describes what Bitcoin has offered.

The reason Satoshi Nakamoto is so brilliant, is that he discovered the secret to getting his idea adopted widely. Satoshi made several clever moves:

- Give everyone a piece of the pie by giving away the software to create more Bitcoins. This is Bitcoin mining.
- Have no central authority, or founder, that controls the currency.
- Make it operate like cash with irreversible transactions.
- Keep the whole system honest and transparent. Everyone has a record of all the Bitcoins, or what is

known as the ledger.

If we move quickly, we can even acquire quite a lot of Bitcoin pie. Already, there are Bitcoin multi-millionaires. After reading this book, chances are many more will join those wealthy ranks. Bitcoin is still just beginning.

Why Should I Buy Or Use Bitcoins?

"Nations are not ruined by one act of violence, but gradually and in an almost imperceptible manner by the depreciation of their circulating currency, through excessive quantity."

Nicholas Copernicus

There are 3 key reasons for getting involved with Bitcoins:

1. Transferring money or value from one Bitcoin user to another (one of the smartest Bitcoins uses)

Here is a comparison chart of the a few methods of sending money and their costs:

Paypal:

As a gift, the transfer is free and limited in amount. Depending on whether an account is verified, the length of time the account has been opened and other variables, the limits can range from about \$100 to \$10,000 in one transaction. Fees will run approximately 2.5%. A \$1000 transaction will net out to \$975 transferred.

Western Union (WU):

Transfers range from \$500 to \$3000 for general transfers and up to \$10,000 for foreign exchange transfers. Fees range from \$5.00 to as high as \$95 for cash pick-up in minutes. Medium range is about \$50. The \$1000 sent by WU will land as \$950.00

Banks:

Wires will run roughly \$30 outbound and \$30 inbound. Sometimes that goes as high as \$50 each way. \$1000 sent via bank wire will result in about \$940.00 transferred.

There are several other digital online currency competitors including Pecunix, BullionVault, GoldMoney, and others. They are not generally used for buying things, but rather for electronic storage of wealth in precious metals.

Bitcoin:

Transfer \$1000 in value through Dwolla.com or even directly through a person to person meeting, for almost no fee. The most a person might pay is approximately \$0.25 when receiving over \$10. \$1000 in BTC value (for today's date that would be about 9 BTC) would land in the recipients account as \$999.75

2. Protecting our wealth by buying into Bitcoins.

This is not necessarily a profitable move. Bitcoins are highly unstable. Prices have risen over triple digits only to fall by 50% in less than 6 hours. (*April 10-11, 2013*)

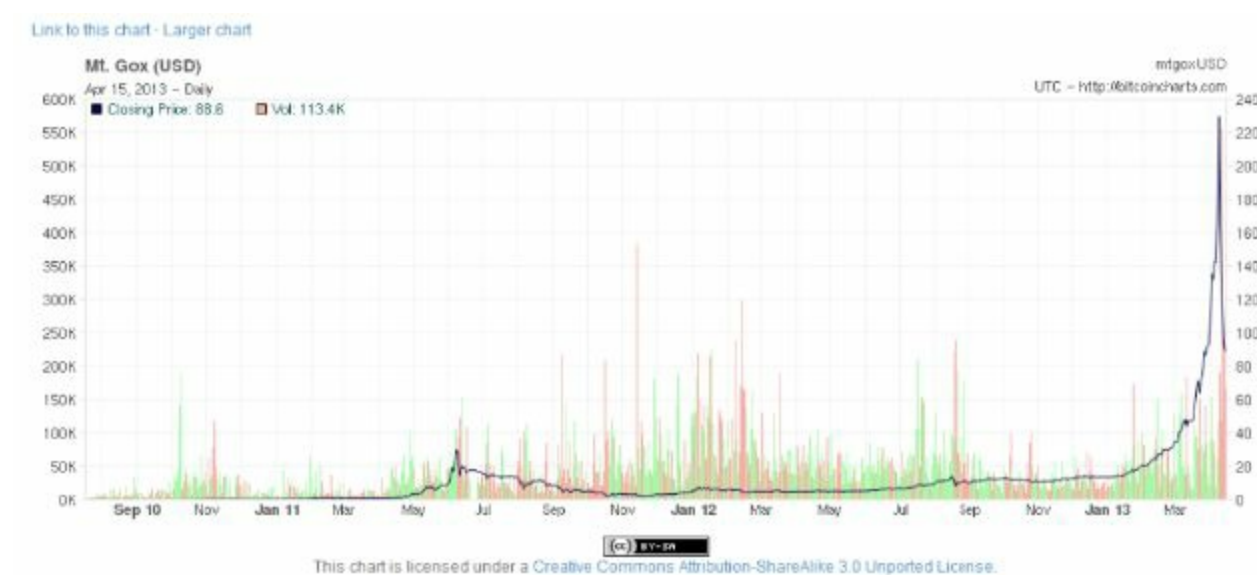
Financial analysts use a term called "beta" for describing the range of an investment. Beta is also

called volatility and relates to the risk of an investment. High beta investments include penny stocks, junk bonds, and some commodities. Low beta investments include treasury bonds, German bonds, etc. Bitcoins fall into the ultra-high beta category. Over time, the beta on Bitcoins will trend toward 1.15-1.5 range. This estimate is based on continued acceptance and greater fungibility.

Variability happens across all markets, including currencies. Only when markets rise as fast as Bitcoin did, do they set-up for a steep fall just as fast.

Bitcoin was designed to offer a limited number of Bitcoins. Limiting Bitcoins through setting how many can be produced is supposed to create a currency that gains value over time.

Here is a chart showing the growth in \$ value of BTC's:



This may be hard to see, but the values ranged from \$.06 up to over \$200.00. While this shows that huge profits are possible with trading Bitcoin, it also shows the possible downside. Storing wealth in Bitcoins at this stage of development is not, in my opinion, the best use of Bitcoin.

The chapter on “How to Trade Bitcoins” is probably a better way to work with Bitcoins. Increasing wealth by simply holding Bitcoins will work better later on. For now, Bitcoins are great for trading, not for storing wealth.

3. Joining the free currency movement and accessing all the motivated customers within it.

Over 600,000 people per month are searching online for how to join the Bitcoin movement. These are potential customers for anyone in commerce. Only a few stores accept Bitcoins currently (see the list in the Appendix). Any store that offers products for sale using Bitcoins taps into a growing market. It does not mean that a store has to only use Bitcoins. They can still accept credit cards, Paypal, or any other form of payment we choose.

Using Bitcoins for commerce and offering products to the growing marketplace brings excitement to

the site, creates back links for improved online rankings, and helps grow the free currency movement.

What Are Bitcoins Really Worth?

Bitcoins, like all currencies today, are worth what they are exchanged for. There is nothing backing Bitcoins. There is no gold, silver, or value of any kind supporting a bottom level for them.

One possible value for the lowest amount a Bitcoin's worth is how much computing power and electricity is required to produce one Bitcoin. This value varies based on electricity costs where the mining computers - that do the work for a Bitcoin reward - are located. Electricity costs for mining a Bitcoin (calculated by PCPer.com here: <http://www.pcper.com/reviews/Graphics-Cards/Bitcoin-Mining-Update-Power-Usage-Costs-Across-United-States>) range.

For a standard Bitcoin mining computer (let's say, an AMD A8-3850 APU), costs range from \$.305 per day to as high as \$2.50 per day. For more specialized computers, the costs range from \$0.55 to \$4.05 per day. The number of Bitcoins produced per day depends on several factors.

The lowest level produced is about 0.050 btc and the highest per computer can reach 3.2 btc. Taking the low end on all numbers gives us a value of:

$(1\text{btc}/0.0050\text{btc}/\text{day}) * \$0.305/\text{day} = \$61.00$ base cost to create or mine a Bitcoin.

The computer's cost is not included here because this level would be for a non-specialized computer.

With a \$/BTC price of \$50 today, each BTC is costing the least efficient miners \$11 to produce. The most efficient miners are still making a lot of money though. Here's a look at more optimistic mining costs:

Taking the high end production numbers:

$1/3.2 \text{ BTC}/\text{day} * (\$4.05 \text{ electricity} + \$8 \text{ computer}) = \$3.77$ base cost for larger scale efficient miners.

Since the \$/BTC exchange rate is \$100+ (and rising) today, a large scale Bitcoin miner can make money all the way down to a \$/BTC exchange rate of about \$4.00

This suggests that rarity is the idea backing Bitcoins. With a BTC production limit of about 21 million BTC occurring in 2140, there is very gradual growth built into the system.

A clear understanding of what inflation and deflation is important. Bitcoin is considered to have deflationary properties. Not so fast.

While on the surface Bitcoins can only reach a level of 21 million issued, with about 12 million currently around, the real story is significantly different. About 100 million times different. Remember the smallest unit of a Bitcoin..the Satoshi? It represents 1/100,000,000 of a Bitcoin. When we total the available units of Bitcoins relative to other currencies, we see that Bitcoins are not nearly as deflationary as they appear.

The real number of Bitcoin units available now is:
1,200,000,000,000,000 or roughly 1 million billion units.

That is not deflationary number. Still, most calculations are based on the 1 BTC unit, and not the smallest denomination. But there is a possibility, as shown above, for Bitcoin to inflate into numbers most of us cannot pronounce. So far that has not happened.

The key thing is understanding what inflation and deflation mean to us in the real world. We can then understand how Bitcoin - or any currency - will behave over time.

Inflation is the amount of money and debt pumped into a system COMPARED TO THE GROWTH OF PRODUCTS AND SERVICES. Notice what has been emphasized. Many analysts focus on the growth of money and debt and forget about the growth of products and services.

The Bitcoin daily growth rate is roughly 0.46% while it decays at a much lower 0.025%. Decaying refers to Bitcoins being used up or disappearing from the pool of available Bitcoins, somewhat like bad debts cause money in a system to disappear. At a net growth rate of 0.44% per day and slowing down, Bitcoins will generally tend to increase in value compared to the large national currencies such as USD, Euro, or Yen.

Here is a critical comparison:

- Bitcoin growth rate is approximately 1.5-2% per year.
- USD monetary growth rate is approximately 5-8% based on ShadowStats.com using the more accurate 1990 methodology and including estimates of M3, the broadest measure of money.
- Euro monetary growth rate has varied from a rare low of 1%, all the way up to 12%, according to the - European Central Bank (ECB) figures. These official figures are almost always understated. The real growth rate of the currency and debt in circulation could be even higher. Typical growth rates are around 5-8%.

(source: <http://sdw.ecb.europa.eu/reports.do?node=100000141>)

CI Monetary aggregates 1)
(annual growth rates; seasonally adjusted)



By checking with the other side of the world, one can find that the Japanese central bankers have been busy! The JCB (Japan's Central Bank) has promised to buy trillions of yen in government bonds. This is almost exactly like printing trillions for eventually pumping into the market place. Prices will rise and potentially explode. The JCB statistics do not show this huge and dangerous monetary growth, with only a 2-5% range of growth rate. The truth will be felt on the street for everyone buying real goods and services in the market place.

This brief currency tour shows that Bitcoins will always be more rare than the competing national and central bank currencies. This fact alone brings value to Bitcoins.

History Of Digital Currencies – And How They Lead To Bitcoin

“Failure is a detour, not a dead-end street.”

Zig Ziglar

Digicash and eCash, YodelBank, 1mdc, e-bullion, ePassport, Liberty Reserve, Liberty Dollar, e-gold, and many others inhabit the museum of former digital currencies. For most of these currencies, they failed from lack of market acceptance. In other cases, such as with e-gold and Liberty Dollar, the banks and governments take them down for being too successful. A charge of money laundering is slapped on the fledgling currency and then the hammer falls.

Understanding the why, who, and what is behind the powerful drive for creating widely accepted digital currencies is the mission of this chapter. Knowing the reasons other currencies went under is critical. If, for example, we know why Digicash disappeared, we can spot the same problem with another currency, such as Bitcoin, long before it loses all value.

Great stock market traders and great investors of any assets have in depth knowledge of the history of their investments. This knowledge enables them to spot trends early both up and down. Using this knowledge they can jump on an up trend early, and off when they spot a downtrend. Sounds basic, right? However, most investors get changes in trends all wrong.

This chapter will help bring anyone up-to-date on the origin of this digital and distributed currency movement. Once the background is understood, one can navigate the future of Bitcoin with greater wisdom, and potentially profit with an accurate assessment of the currency.

Digital Gold, Silver, False Promises And Digital Scams

Digicash, later acquired by eCash, could be called the parent to the idea behind Bitcoin. David Chalmers, a brilliant programmer and cryptographic expert (cryptography is the math study focused on creating codes that are difficult or impossible to break for securing data), founded this digital currency. His ideas worked with some of the same concepts for creating online payment “tokens” similar to Bitcoin.

Digicash went bankrupt in September of 1998, although it had been more of a promise of major electronic currency, than a reality. With multiple failed business deals from Visa, Microsoft, ABN AMRO, ING and others, Digicash was unable to gain market traction.

According to an article about the demise of Digicash in NEXT! Magazine, January 1999:

“The dogma of Chaum, that DigiCash should aim for the virtual world, was abandoned. It was no use trying to compete against the credit card companies; they would squash you if you upset them. “

David Chalmers repeatedly ruined market joint venture agreements by insisting on too much money and too much secrecy. Digicash and eCash died through mismanagement partly, and competitors that realized it could eat their lunch.

Lesson #1: A digital or alternative currency needs to partner early, often, and profitably to survive and grow.

Knowing this historical lesson, anytime we see Bitcoin gaining a significant store, business, or website as a user, it is time to load up!

A great showcase of this effect occurred between December 2012 and February 2013. Wordpress.org started accepting Bitcoins, and the first Bitcoin bank (Bitcoin-central.com) opened up. Bitcoin rose from under \$20 to over \$34 in this period.

After Digicash and eCash went away, there were hobbyists that kept working on the concept for a new digital currency.

Something old and something new came together first, however, and e-gold hit the market. A Florida doctor and his computer savvy partner came up with a precious metals backed electronic currency. Unlike Bitcoin or eCash, real gold and silver backed up the value of e-gold.

e-Gold eventually reached a user base of over 5 million. While it used sophisticated encryption for handling transactions, it was a centralized currency. This is what ended up killing e-gold.

The U.S. government accused e-gold and its founder of money laundering and other crimes. E-gold was soon finished. Even though the e-gold system still exists, it is no longer a live e-currency.

Lesson #2: Any alternative currency with a central office, authority, or person will be shut down, jailed, or destroyed by a government and/or bank.

Even when the new alternative currency has no similarities with U.S. currency, the government will accuse the currency producer or promoter of the crime of counterfeit under Title 18 section 471 of the

United States Code. Being found guilty results in a 20-year sentence (approx.).

Bernard Von NotHaus, founder of the Liberty Dollar, was convicted in 2011 of “making, possessing and selling his own currency.” People who bought the Liberty Dollar made a lot of money with his currency. It was silver backed, beautiful, and began to gain acceptance.

Anne M. Tompkins, a prosecuting attorney during the trial in Western North Carolina described the Liberty Dollar as "a unique form of domestic terrorism" trying "to undermine the legitimate currency of this country"(New York Sun, March 2011).

The jailing of a person founding a currency explains one of the reasons why the founder of Bitcoin is largely a secret.

Lesson #3: Any person controlling a popular alternative currency will become vulnerable to legal actions sooner or later.

Who Hates Bitcoin And Why?

As we have seen during the brief history of alternative currencies on the Internet, they often fail spectacularly. Governments have a monopoly on currency. Banks have a monopoly on storing, distributing, transferring, making loans, and exchanging currency.

Governments want to tax anything and everything. That is what they do best. Taxing transactions and people requires knowing who spends what and with whom. Any alternative currency that offers anonymity such as Bitcoin, presents governments with a hard challenge.

How can they track Bitcoins and the users to tax them?

If we set-up our Bitcoin accounts in a certain fashion, and do not bring Bitcoins back into our bank accounts, then governments have a hard time of accessing this information. Banks look at Bitcoin as an enemy stealing their wire fees, currency exchange fees, late fees, overdraft fees, and even their bank vault fees. Banks of all kinds, governments around the world, and the centuries old power structure of world banking families and institutions all hate Bitcoin.

While they may hate Bitcoin, we can also be sure they are involved.

Recently, an individual slammed the value of Bitcoin by selling a huge quantity in less than one hour. Mtgox.com, the major trading exchange for converting and trading Bitcoins, shut down for over 12 hours. This caused Bitcoin value to plummet because nobody could get their value in their national currency out of Bitcoin. Almost like a bank closure, termed a bank holiday, Bitcoin experienced a triple digit to almost zero value in less than a day.

Some theorized that this was a test run by banking and financial powers, backed with government approval, to see how they could ruin this new competitor. While a banking entity or government crashing Bitcoin is a possibility, a private individual can crush any currency in similar fashion. George Soros famously helped devalue the British pound in September 16, 1992. Soros sold British pounds aggressively which he had borrowed, and eventually forced the Bank of England to break it's peg to the European Exchange Rate Mechanism. Soros made over \$1 billion in this trade.

Unfortunately for most Bitcoin users, they all lost money when the mega seller struck. One of the main portions of this book will help readers avoid that waterfall plummet in value. Not losing money is the first rule of investing and trading.

Why Bitcoin Is Different And Better Than Everything – Almost.

Since nobody owns Bitcoin, it is hard to shut down. With thousands of people creating Bitcoins in what are called mining operations, there is every incentive for people to get involved. Profit brings participation. The software running Bitcoin is open source. Everybody can see the code, comment on it, and verify that it is legitimate. Developers gather in several places online, but the main hub is: <https://github.com/Bitcoin/Bitcoin>

Compared to previous digital currencies, and standard currency, Bitcoin has several amazing advantages:

1. Anybody can get involved in mining Bitcoins or creating currency. This is almost like being a gold or silver miner. It costs money to get set-up mining Bitcoins, and it gets more difficult every day, like the real world of mining.
2. Every node in the Bitcoin network knows about all Bitcoin transactions and keeps the ledger of the currency. This transparency keeps the system honest. No one can spend the same Bitcoin twice because each Bitcoin is checked throughout the system.
3. Bitcoin availability is limited. Earlier we saw how the central banks around the world (i.e. JCB) can create trillions in national currency in an instant. Money creation at that level makes national currencies become worth less over time. Bitcoins get created at a steady and diminishing rate. This results in a currency that gets more valuable over time.
4. It is possible to operate completely anonymously with Bitcoin. This is getting harder and harder to accomplish. We cover this in detail later in the book. It is a good idea to get set-up as an anonymous user as soon as possible. The anonymous window will close - and soon. Do not worry about setting up a Bitcoin account tied to your identification. We can do that any time. We can also set up as many Bitcoin accounts or identities as we want.

While some other currencies, notably e-gold, offered some privacy, all the records could be tracked back to the e-gold website. Additionally, all the ID's of users stayed on the e-gold servers. They were eventually confiscated during the federal raid. Many of the records for supposedly private, anonymous parties were turned over willingly by e-gold. Short version: centralized currencies cannot guarantee privacy completely. Bitcoin makes a good attempt at this, by distributing all transactions without needing one clearinghouse or one central database.

5. Bitcoin has no counter-party risk. It is mathematically proven and backed. Counter-party risk comes from someone or something backing a currency or certificate.

The US dollar has the definition in the constitution of:

24.057 grams or 371 4/16 grains of pure silver as set out by Secretary of the U.S. Treasury Alexander Hamilton in 1792.

Now, the dollar cannot be turned in to a U.S. bank for silver. The counter party for the value of the U.S. dollar is the U.S. government. Our government has broken it's own law and will not give the

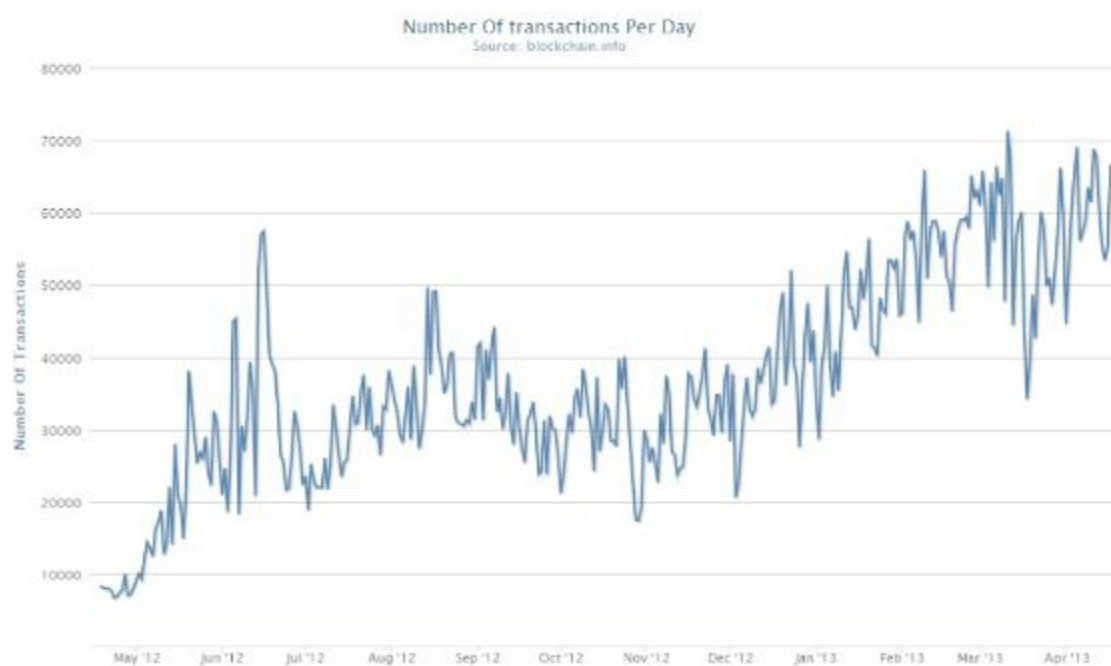
value defined by the dollar.

Bitcoin has no counter-party backing it. There is no risk of default on what a Bitcoin is worth. Almost all other digital currencies that are backed by gold or silver, have a significant counter-party risk.

6. We can store Bitcoins in our brain, by memorizing key codes that define our access to Bitcoins. Other currencies prevent this because there is a central clearing house. Even a correctly memorized code will not work if the central clearing house or controlling monetary authority denies access to the account. This denial of account status just happened in Cyprus, and even occurred with the U.S. bank holiday during the depression. As long as the Bitcoins check out as legitimate against the Bitcoin ledger, they are valuable for Bitcoin transactions. No one can stop the spending of them.

7. Bitcoin is robust and resilient. Software programmers apply words such as robust, resilient, error tolerant, and self-healing when referring to code or systems that are hard to break. Bitcoin can only be stopped for good by destroying all networks, computers, and exchanges. When and if that happens, no one will be worrying about Bitcoins; we'll be in much deeper trouble.

Spread out across the globe, across all computer networks, with a steady up trend in use, and proven code, Bitcoin has staying power. This chart from Blockchain.info shows the general up trend in Bitcoin transactions. Nearing 80,000 transactions per day currently; when it tops 100,000, there will be a sudden upsurge.



8. Bitcoin creates businesses. None of the other alternative currencies created sites with as much traffic as MtGox.com. Bitcoin has already surpassed every prior virtual or digital currency with its popularity and price increases. While e-gold grew to over 5 million accounts, the number of significant stores accepting it never grew over the 100 mark. Bitcoin already has a steadily increasing list of merchants that accept Bitcoin; one list of merchants working with Bitcoin is here:

<http://www.Bitcointrading.com/forum/spend-Bitcoins/online-stores-accepting-Bitcoins/>

9. Bitcoin transactions are irreversible. Unlike credit cards, a buyer who transfers funds to a seller cannot reverse the transaction getting their money back. Once we send Bitcoins, they are now gone. Getting our Bitcoins back, or reversing our spending of them, requires the seller or receiver of the Bitcoins to start a new transaction for sending back the purchase amount.

While we might consider this bad news, it shares this characteristic with cash. When we hand over cash buying something, we cannot reverse the transaction. The receiver of the cash has to agree to return our money.

Irreversibility turns out to be a positive for buyers, though they may not recognize it. When businesses accept credit cards and payment forms such as Paypal, they have to add somewhere between 5%-15% to each price for return allowances and scams. This fee is on top of the 3%-5% that credit cards, Paypal, etc. charge for their service. Total punishment that most buyers do not consider, but nonetheless pay for: about 8%-20%.

Cash-like transactions - irreversible ones - can result in reduced prices (*can*, but not necessarily will).

For sellers, usually businesses accepting Bitcoin, this irreversibility property solves one of the biggest problems with credit cards and Paypal.

For buyers, sometimes the lack of reversing transactions may not be a good thing. Some creative entrepreneurs realized this buyer concern was an opportunity for an escrow service.

Here are a few Bitcoin escrow services:

<http://www.btcrow.com/>

<http://www.thrucoin.com/>

<http://www.clearcoin.com>

Escrow services hold funds until the buyer agrees that the seller delivered. There are also dispute settlement operations included, though not where a seller wants to get involved if at all possible.

Other digital currencies have offered irreversibility, though without the convenience of escrow services. If we send a Western Union payment, it is gone essentially. There are no integrated Western Union escrow services.

10. Bitcoin's entrenched user base with about four years of operational proof gives it market dominance. There are other digital currencies, such as Pecunix, PerfectMoney, Liberty Reserve, etc. that have been around longer. However, none of the competitors have the explosive user base, nor do they have the growth trend of Bitcoin:



Globally, there are about 900,000 searches per month on Google for Bitcoin. While the crash in April 2013 slowed search traffic, there are still well over 800,000 unique searches per month, with over 50,000 new mtgox.com accounts added per day at the peak. Mtgox is the biggest Bitcoin exchange and a good indicator of BTC popularity.

There are many other differences between Bitcoin and other digital currencies. Understanding these differences requires going into the intricacies of how Bitcoin operates. We will venture into more of a technical look at Bitcoin in the remaining chapters. When we learn how Bitcoins get created, spent, saved, and circulated it will give us the keys to creating our own wealth with Bitcoin.

How To Use Bitcoins

“Tell me and I'll forget. Show me and I may remember. Involve me and I will understand.”

Chinese Proverb

This chapter will get our Bitcoin running shoes on and get us into the race. We will examine where and how to get set-up with Bitcoin, and look at best practices when doing so. We can set-up multiple Bitcoin accounts and wallets. If we make a mistake or want to create a separate Bitcoin wallet or key, we can do that easily.

Getting Your First Bitcoin

Mining is one way to acquire Bitcoins, but not practical for getting them immediately. There are a few sites we can use for setting up our Bitcoin money system.

There Are 3 Basic Needs When Starting Out:

1. A Bitcoin Wallet

We can hold our Bitcoins or Bitcoin codes on our computer, USB drive, SIM card, or our iPhone or Android phone. If we lose the computer or device somehow, those coins are gone also. Not desirable.

We can secure our Bitcoins by signing up for a Bitcoin wallet that resides in the Internet cloud. We then back-up the information to our phone and/or computer with encryption, and then distribute that encrypted information. Only we will hold the key, or those we trust, for unlocking our Bitcoin wallet information. This will all become clear when we get through the simple, almost instant process.

A Bitcoin wallet gives us a Bitcoin address. When we buy or sell Bitcoins, we use this address. Here is a Bitcoin wallet address set-up with Coinbase.com, one of several Bitcoin exchanges and wallet providers:

1Lez1wcwPLWNmPtcfGXtSy8F34ZF45fwYh

We will probably end up having many wallets and many bitcoin addresses. Recommended practice is to have one wallet address for buying Bitcoins and one for selling them.

Here is a view into the account of this new Bitcoin wallet with no Bitcoins. This is a new Bitcoin wallet without any bank account attached to it, or fully operating. We could receive Bitcoins with this address, but we will need to link a bank account to transfer money in for buying Bitcoins.

Transactions

Buy/Sell Bitcoin

Linked Accounts

Merchant Tools

Account Settings

Invite your friends to Coinbase

Just [Tweet](#) this link or copy and paste this url below into Facebook to invite your friends to try Coinbase:

[Read more](#)

Linked Accounts

Verifications and Limits

Bank Accounts

used to buy and sell bitcoins, U.S. only right now

+ Link A Bank Account

[How is my information protected?](#)

Bitcoin Addresses

used to receive bitcoin from external sites

1Lez1wcwPLWNmPtcfGXtSy8F34ZF45fwYh

Copy Address

created less than a minute ago

+ New Bitcoin Address

[View All](#)

Here is just a partial list of Bitcoin wallet providers that store our Bitcoins in the cloud with back-up options:

- <http://www.Instabit.com>
- <http://www.Blockchain.info>
- <http://www.Coinbase.com>
- <http://www.walletbit.com/>
- <http://instawallet.org/>
- <http://www.dwolla.com>
- <http://www.myBitcoin.com>

There is another alternative way of getting a Bitcoin wallet - though it is much more than that. One can sign up with OkPay.com, which offers more of a banking-like service level and direct transfers of funds to a debit card. The risk with OkPay.com is that it has more financial liabilities than the other Bitcoin wallets mentioned.

Setting up an account with OkPay.com is good for getting funds out of Bitcoins more easily. It is not the most secure place for getting a Bitcoin wallet because of the financial liabilities inherent with their wide transfer offerings.

There are several Bitcoin wallets that we can set-up on our computers without access through the Internet:

- Electrum
- The Satoshi Client
- Armory
- Multibit

These local computer based Bitcoin wallets are more complicated to use and keep secure. For most users, a Bitcoin wallet with Blockchain.info (Internet/Cloud Hosted Wallet) will be their best choice.

2. A linked account for funding Bitcoin purchasing

This is usually a bank account. We have to go through verification steps that can include tracking small deposits that the Bitcoin wallet provider may make to guarantee we own this account. Paypal uses this method. Plan on a 24-72 hour wait for this process.

3. Our first Bitcoins or bitcents

We can buy from the same place where we signed up for our Bitcoin wallet. We can also get Bitcoins locally. LocalBitcoins.com is a marketplace for buying and selling bitcoins locally with cash and other payment methods of your choice. You can find a local bitcoin trader near you or can even start your own bitcoin exchange to sell your coins. This is one of the most interesting aspects of this system. Unlike the current, formally appointed exchanges, anyone can become a Bitcoin exchanger and offer their own rates of exchange.

More commonly, people go to the largest of the exchanges, Mtgox.com, and sign up for an account

there. We can then use our Bitcoin wallet address for buying Bitcoins on the Mtgox.com exchange. Once we have funded the Bitcoin wallet provider from our bank account (Coinbase for this example) we can then buy Bitcoins - possibly.

Buy Bitcoin

Sell Bitcoin

History

Note! We've exceeded our normal buy limits for today. If you would still like to purchase you will receive the market price of bitcoin on Monday Apr 22, 2013 at 12:27PM PDT after your funds have arrived. [read more](#)

Buy approximately BTC (current market price is \$88.93)

Debit my U.S. bank account [link and verify a bank account](#)

Subtotal	\$0.00
Total	\$0.00

You'll need to [Link And Verify A Bank Account](#) before you can buy bitcoins on this page.

Look at this shocking screen:

Coinbase has reached their daily limit of buying Bitcoins for their clients, us. This happens frequently in the Bitcoin world. With only a small number of Bitcoins in circulation - far less than the 11 million already produced - there is more demand than supply. This lack of supply results in people not being able to get any Bitcoins at times. Eventually the price per Bitcoin rises for the buying/selling pressure to equalize.

Spending Bitcoins

Assuming we were able to get Bitcoins for our new wallet, we will have our Bitcoin wallet, Bitcoin address, and some Bitcoins. We can now spend these Bitcoins in similar fashion to other spending processes. However, it is harder to find a store or service that is offering what we want in exchange for Bitcoins. Here's one of the longest lists of online stores that currently accept Bitcoins: <https://www.spendBitcoins.com/places/> (Appendix 4 lists these stores)

The other alternative for using Bitcoins, is person to person commerce. Any person we find on craigslist, ebay, or any auction site may allow using Bitcoins to complete the transaction.

A Bitcoin transaction for a buying from a store looks like this (<http://the-chocolate-tree.bit-trade.co.uk>):



As with any other form of payment, we have to fill out the usual our name, phone, address and delivery information before getting to the payment screen:

Order Information

0.8600 BTC

Order Number: 53

Valid for: 14 m : 48 s

Pay this Invoice

Scan to Pay



Click to Pay

Only for use with
URI-compatible wallets.

Send 0.8600 bitcoins to:

151007sfhfzruk7ba3ibNkv5EW7rKLSEA



This is a one-time use bitcoin address. Do not store this address for future payments.

2019/04/17 20:14:30 GMT



There is a time limit for this screen and the Bitcoin address provided of about 15 minutes. We have 15 minutes to send money by one of two ways for our purchase. If we have our Bitcoin wallet client loaded on our computer and it has what is called the “URI-Compatible” wallet running, we can press the “Click Here” button and instantly send the Bitcoins from our wallet to the chocolate store. URI-Compatible wallets include: Blockchain.info, Armory, Bitcoin Wallet, Multibit Spinner, and a few other smaller players.

The QR code - of black and white blocks in the center- is for scanning our phone and paying with a smart phone loaded Bitcoin wallet.

The most common and simplest way is using the long and unique Bitcoin address for sending the payment. To send Bitcoins via email from our Bitcoin wallet address to the chocolate company for this purchase, we must go to our Bitcoin wallet. Here, we go to our wallet on Coinbase.com and head to the page for “sending money”. Depending on where you have your wallet located, it may appear a bit different than the image below. However, they all have a send money screen that is similar and operates almost exactly the same way:

Send Money

To:
enter an email or bitcoin address

Amount: or

Notes:

inn • Network • Legal • Jobs

1518B7sFhfZzuk7ba3JbiNkv5EW7rKL SEA

In the “To:” section we put the Bitcoin address of the chocolate company, which they’ve listed, on their buying screen. Cut and paste the Bitcoin address in, and then set the Bitcoin amount of 0.86 btc for the price of the chocolates. Hit send, and chocolates are on the way!

Important to note, there can be a delay time of around 10 minutes for the merchant or seller to accept your purchase. Generally, this delay of 10 minutes just applies to the computer and phone-based Bitcoin wallets. The merchant has to confirm that the Bitcoin spend is legitimate by checking around the network of all Bitcoin holders. Online wallets generally provide instant recognition of Bitcoin spends or sends.

There are other ways of spending Bitcoins. There can be bulk sends, donations, and escrow versions. Each system of wallets and exchanges has slightly different ways of spending Bitcoins.

For sending donations or tips, the format in forums and other systems looks like this:

+Bitcointip @Username \$1usd

Sending tips, donations, bulk payments, can all be handled through Bitcoin wallets instead of memorizing codes.

Saving Bitcoins

We started saving in Bitcoins the minute we transferred money and bought Bitcoins for our wallet. We have become our own bank. We will not gather interest by just holding Bitcoins in our wallets, but we will probably see the value of our Bitcoins rise every year on average (versus our national currency).

When using Bitcoins, our expectations for how we receive, save and spend money has to change slightly. We have all the power of a bank with our Bitcoin wallet. We do not depend on a bank for confirming that there is money in our account. Bitcoin handles this automatically. We are completely free of the government FDIC system and the banking system, for the better according to most Bitcoin supporters.

What about collecting interest such as banks, credit unions, and financial institutions offer?

There are Bitcoin banks popping up that offer Bitcoin interest: Flexcoin.com offers an unknown quantity of Bitcoins monthly based on average account balances. It also acts as a Bitcoin wallet.

By now, a reader could be understandably confused about the difference between having a Bitcoin wallet and some of the services for Bitcoin. Confusion is a hallmark of any new technology. For now, the important tip is that we Bitcoin users will have multiple Bitcoin wallets, with multiple Bitcoin addresses at different sites for different wallets, and use different exchanges (mtgox.com, localBitcoin.com, etc.) as we wish.

Unlike the challenge of opening new accounts forced on us by banks, Bitcoin allows us to have as many wallet addresses as we wish. This helps maintain our anonymity. One Bitcoin wallet can have many Bitcoin addresses. The Bitcoin applications we decide to use keeps track of all of this for us.

Investing In Bitcoins Or Not

Buying a Bitcoin is a form of investment. Buying Bitcoins also works almost like a foreign currency trade. We “sell” our national currency - USD, Euro, GBP, Yen, etc., and “buy” Bitcoins at the same instant. The huge difference between foreign currency investing and Bitcoin, is that there is almost no friction cost to the trade.

Fees for buying and selling currency can be steep. Buying Bitcoins or selling Bitcoins for a national currency is almost completely free of any fees. The big cost is the Bid and Ask spread, or the difference between what people will pay versus what people are asking for a Bitcoin.

Opening a foreign currency, commodity, stock, or any investing and trading account can be a hassle. We often have to prove income, net worth, years of experience trading, credit score, and other private details. Bitcoin investing offers a smoother, easier, and simpler way to invest.

Buying and selling Bitcoins offers foreign currency investing profit and loss opportunities. Already the early adopters of Bitcoins have multiplied their net worth many thousand fold. Those who bought Bitcoins around \$5/btc around early to mid 2012, are now sitting on almost 20 fold profits in less than a year.

More sophisticated investors can buy derivatives (similar to options in the stock and commodities world) from two new exchanges: iCBIT and with the IG Group. Neither of these markets are being heavily traded thus far.

There is also a Bitcoin mutual fund of sorts, based out of Malta. Primarily for institutions and high net-worth investors that want Bitcoin portfolio exposure. At the moment, this is not a recommended approach for buying.

While admittedly risky, the upside for investing in Bitcoins is life-changing gains.

The “How to Trade Bitcoins” section of this book explains techniques for extracting the most profit out of Bitcoin investing. Bitcoins are not yet accepted for buying shares on national stock markets. This situation is unlikely to change anytime soon. Banks and governments controlling commodity, stock, bond and currency trading exchanges will not want to cede credibility to Bitcoin.

No matter, even without access to any conventional investing markets, Bitcoin has the potential for vastly outperforming other investment classes over time.

Protecting Bitcoins

Protecting our Bitcoins is critical. It has the same critical importance as protecting cash, gold, bank account access, or any easily converted item of value. Bitcoins can be stolen the same way a password can be stolen, or an online account for email can be hacked and abused.

There are several ways for protecting our Bitcoins:

1. Keep our Bitcoins in our online web wallet at anyone of a number of sites

So long as we keep our login credentials secure, the main risk is that our wallet site will be hacked. InstaWallet was hacked and closed on 4-3-2013.

2. Keep our Bitcoins on our computer or cell phone

This ups the risk of loss because computers and cell phones can be stolen. While we may have a password-protected device, passwords can be broken, and we lose access to our wallet when our device is stolen. Whether or not the criminal gains access to our Bitcoin wallet on our device, we lose access.

If we do want to keep our wallet on our computer or cell phone, it's suggested to use TrueCrypt for encrypting Bitcoin files such as wallet.dat.

Keep two wallets for using this protection system. One wallet has a small amount of BTC's for daily use and the other is like a savings account with more BTC's. The daily use BTC wallet will not be encrypted so it is easy to use daily. TrueCrypt will be used for the savings wallet for protecting the greater store of BTC's. This way, if our computer or device is stolen, we only lose the small wallet of BTC's. Our big savings stash of BTC's will be secured with 256-bit encryption.

We can encrypt all our Bitcoin files, wallet addresses, passwords, and our account ledger. We then load these encrypted files onto a secured USB drive, SIM card, or any storage device such as an MP3 player.

Once all our files are encrypted with TrueCrypt (Truecrypt.org) or similar tool, we can safely distribute those Bitcoin files and addresses to anyone for back-up purposes. Only we will have the password for cracking open the TrueCrypt files and using the Bitcoins.

3. A hybrid of #1 and #2.

Use an online version of a Bitcoin wallet for our daily spending with normal password protection and then store the major portion of Bitcoins on our computer or cell phone with the full TrueCrypt protection and distribution explained in #2. This is the ideal method. Having our Bitcoins in an online wallet, especially Blockchain (at <http://www.Blockchain.info>) brings a more convenient experience. We can send money as long as we have Internet access either on a phone or computer, anywhere, any time. Blockchain's wallet excels in cross-platform performance from on-line, off-line, iPhone, Android, or locally stored computer applications.

This last method of protecting our Bitcoins bridges the convenience vs. security gap with the best of both worlds.

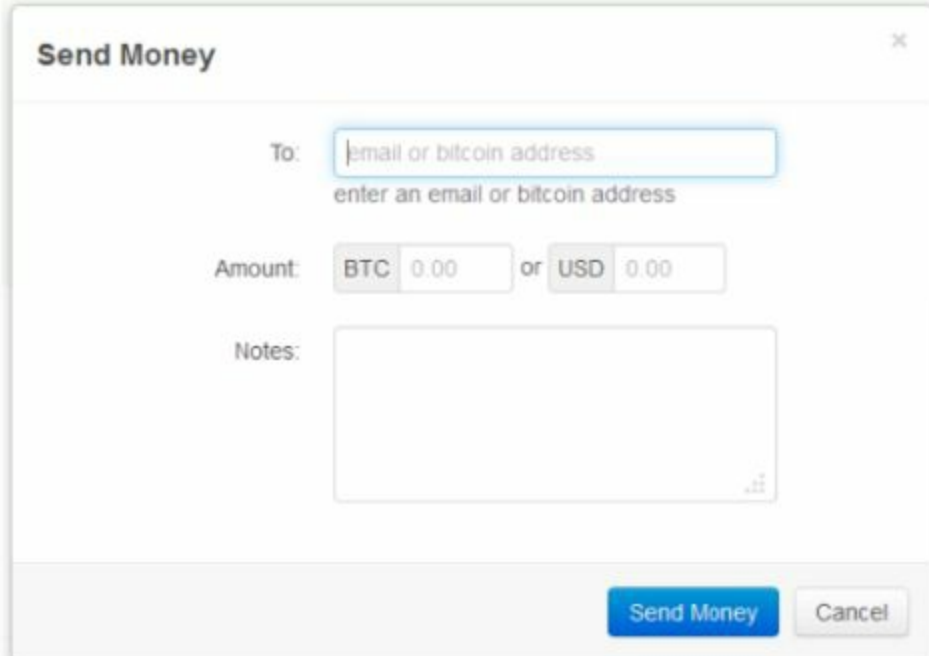
Transferring Bitcoins

Transferring Bitcoins is almost exactly like spending Bitcoins shown in a previous section. When transferring Bitcoins, we normally do not have a time limit such as in the chocolate purchase example. Also, there is usually no limit to the amount in Bitcoins we can transfer. Different wallets and exchanges have limits on who and how much can be transferred. Some wallets require proof of age for transfers and accounts. Coinbase requires users to be 18 or older.

Bitcoin wallets stored locally will be free of such limits. In-exchanges, where we fund our Bitcoin purchases, often limit the amount of national currency we can convert into Bitcoins. Some limits apply based on the laws followed by particular exchanges. Mtgox.com limits transactions to roughly \$1000 per 24 hours. Other exchanges, such as Bitcoin-24, have no limits on transactions or withdrawals.

There is no limit on how many Bitcoins we can send from our Bitcoin wallet to any other Bitcoin wallet. That is a direct transfer. However, if we choose to go through an exchange, limits may apply.

Sending a transfer looks exactly like the Send process shown earlier. We simply ask the receiving party for their Bitcoin address or Bitcoin wallet and put that piece of code in the Send space as shown below.



The image shows a 'Send Money' dialog box with a close button (X) in the top right corner. It contains three main input fields: 'To:', 'Amount:', and 'Notes:'. The 'To:' field has a placeholder text 'email or bitcoin address' and a hint 'enter an email or bitcoin address' below it. The 'Amount:' field has two sub-fields: 'BTC' with a value of '0.00' and 'USD' with a value of '0.00', separated by an 'or' label. The 'Notes:' field is a large text area. At the bottom right, there are two buttons: 'Send Money' (blue) and 'Cancel' (grey). Below the dialog box, there is a breadcrumb trail: 'Home > Network > Local > Jobs'.

Note that we can also use an email address. The person receiving this Bitcoin Send will get an email from Coinbase explaining they have Bitcoins waiting for them. They can either provide Coinbase a Bitcoin wallet for receiving the payment, or set-up an account with Coinbase for receiving the payment.

There are many other ways of sending Bitcoins directly to debit cards with OkPay.com, or to other online payment services with Dwolla.com, MyBitcoin.com, and others. Same basic steps apply.

1. Get the receivers Bitcoin wallet address.

2. Open our Bitcoin wallet or account screen on any Bitcoin exchange we have our Bitcoins stored in.
3. Use the Send function and put the receivers Bitcoin address and/or email in the “To:” box.
4. Carefully confirm amounts and addresses. Once we hit send, there is usually no method of canceling or recalling the transfer.

Accepting Bitcoins In Business

Bitpay.com appears to be the leading merchant services provider for online stores. There are several other methods that work almost like Paypal for accepting payments via Bitcoin. The other Bitcoin merchant tools do require some custom coding.

All we need to do is give users our Bitcoin wallet address for sending payments to us. We can also choose to create an individual wallet address for each sale. This is how the automatic checkouts work and requires software for generating an unlimited number of unique Bitcoin wallet addresses.

Bitpay.com simply requires setting up our products with BTC prices, the normal account tie-ins such as business name, tax code number (EIN# for a business or Social Security# for individuals in the U.S.) and accounts tied to the BTC wallets. Then Bitpay provides all the clearing and collection function.

Showing that we accept Bitcoins on the first page of our store or site shows we are ready for conducting business in the newest digital way.



With our proud sign displayed, we can use one of many different merchant solutions. Bitpay is generally the leader, but others offer similar functionality.

Merchant solutions for Bitcoin:

- Okpay.com
- Mtgox.com
- BIPS
- BitUtils
- Paysius
- Walletbit
- Bitpay

This is only a small portion of the ever-expanding options for merchants.

All that we need to do to sell with Bitcoins, is sign-up for one of the above accounts, (again, bitpay.com is recommended) and place the correct Bitcoin code they provide onto your website. The site will automatically coordinate the Bitcoin transfers and loading up the correct wallet from the purchases.

Using Bitcoins Anonymously

There are several forms of anonymity for online purchases.

Store/service purchasing transaction anonymity - We are able to generate separate wallet addresses so that the store does not see repeat orders from one wallet. This form of privacy breaks the database many stores, such as Amazon, Target, Costco, etc. keep on customer purchases. There will be almost an infinite number of purchases from different Bitcoin wallet addresses. Different Bitcoin addresses with different purchases makes it almost impossible to track buyers.

We can maintain this low level of anonymity by creating a new Bitcoin address or wallet for each purchase. Many Bitcoin wallet services or clients have a “New Address” option for each purchase. This option creates a shadow wallet address that ties in with your main wallet and masks where the purchase came from.

Our original Bitcoin wallet address, account, and email address can be tracked back to our Internet service provider (ISP), computer, and finally, our identity.

Preventing any attempt at linking a person to a Bitcoin wallet address, service, or email requires a more thorough approach.

These steps are available from Anonymity.com:

1. Use Tor browser from <http://www.torproject.org>.
2. After Tor confirms that you are being routed through the Tor proxy network, go to TorMail for hidden service and create an email account. This is the first, and major roadblock for anyone tracking Bitcoin addresses - anonymous email addresses.
3. Create a new, anonymous email address through Tor for each new Bitcoin purchase.
4. Use the bitinstant.com service or others that allow cash deposits for Bitcoin to email purchases. Another option is to use localBitcoins.com for buying them in cash anonymously.
5. Use the created TorMail email address, the amount of money you are converting to Bitcoins, create a name with a DOB. Will be a good idea to keep these handy, but not necessary.
6. Take the cash deposit slip to the service counter that completes the deposit process. There may be cameras to avoid at some locations.
7. The transfer will be completed after you get confirmation, normally within an hour. Create another Bitcoin address using the same steps above, and send the Bitcoins to the newest address created with TorMail.

Following these steps creates a nearly impenetrable wall of anonymity.

Our anonymity is not fool proof with Bitcoin. Most of the services commonly used, such as Dwolla, MtGox, Bitcoin-24, Flexcoin, and many others do require tying our account to bank accounts, and often cell phones. This account linkage requires much more effort for clearing our trail. Getting a prepaid phone from a small retailer in the \$20 range, we can receive our confirmation text with this phone and not use it for anything else.

Getting funds into and out of the Bitcoin wallet for everyday use will have to occur without having a bank account tied to the Bitcoin service. Once we tie our bank accounts in, we have lost anonymity.

Paypal is not a popular method of buying Bitcoins, partly because it breaks anonymity. The other reason for avoiding Paypal, is that there is up to a 7 day delay for obtaining Bitcoins through Paypal. This delay stems from the reversibility of Paypal transactions. Avoid using Paypal because other Bitcoin users will suspect the transaction to be spam or from a dishonest person.

Our options for fully maintaining Bitcoin anonymity throughout - and not on a per transaction or per store basis - necessitates buying Bitcoins with cash, barter, silver, gold, or anything but bank wires, debit cards, Paypal, or standard financial instruments.

How To Create Bitcoins Or Become A Bitcoin Miner

“No one has a right to consume happiness without producing it.”

Helen Keller

Early on with Bitcoin, simply downloading the Bitcoin software started us on the road as Bitcoin miners. We started the software for Bitcoin, and it would show how our computer processor was mining Bitcoins as it solved the cryptographic code-breaking problem. It was a slow process for earning Bitcoins on normal PC's.

More powerful computers could dramatically increase the rate for solving the puzzles or hashing as it is referred to in the Bitcoin lexicon. The creator(s) of the software anticipated that Bitcoin mining would go big. The software code and mathematics creates more difficult problems to solve - or mine - as the number of Bitcoins in circulation increases.

The Concept Of Bitcoin Mining

Gold and silver are mined into existence. Costs for finding, licensing, mining ore, culling ore from gold and silver, then minting coins and bars, creates a value for gold and silver. Bitcoin has a similar set-up, though not as costly or involved. The key difference is that mining for Bitcoins involves solving codes or cryptographic mathematical puzzles.

The most important aspect of mining Bitcoins, is that anyone can get involved. There is no central bank, no government treasury, no board room filled with supposedly all knowing people deciding how much money to produce. We can all produce Bitcoins, provided we can set-up a mining operation.

Terms BTC Miners Use:

Mining - Solving the math puzzles for generating the next block. Miners hash at a certain rate based on computing power and the difficulty of the Bitcoin hash over time.

Rig - the complete set-up for solving the Bitcoin algorithms involving power source, processing unit, code, input and output controllers. These are normally dedicated Bitcoin servers, but could be any form of computer or graphics card devoted to solving the BTC block puzzles. This involves a red-hot fast CPU, GPU (Graphic Processing Unit), ASIC (Application Specific Integrated Circuit), and now dedicated computer boxes called FPGA. Field Programmable Gate Arrays are taking the speed championship from ASICS for cracking codes.

Hash Rate - The speed a rig can solve or make calculations for the Bitcoin network. It is expressed as TH/S for Trillion Hashes/Sec or GH/S for Giga Hashes/Sec.

Block - A record that confirms many waiting transactions. It then becomes part of a block chain where each block relates to previous and future blocks through agreement of code segments.

Block Chain - A grouping of blocks forming the public record of all Bitcoin transactions in chronological order. It is shared among all Bitcoin users for verifying the false from true Bitcoin spends, the balance of Bitcoin addresses, and prevents double spending of Bitcoins. Think of the block chain as the ledger for Bitcoin, with encoded entries.

Bitcoin - These are unique codes “awarded” to miners for solving the problems that allow for creating the next block in the block chain. Bitcoin was awarding 50 Bitcoins per solution and now is awarding about 25 per solution. This will go down to 12.5 Bitcoins per block in 2017. Every four years the number of Bitcoins created per 10 minutes will go down by half, until 2139.

How To Mine Bitcoins

For learning about mining (and not creating any Bitcoins for a long, long time):

1. Visit - <http://www.Bitcoinplus.com/generate>
2. Click “Generate”
3. Watch as your computer begins solving the Bitcoin codes - and makes almost no progress over time.

BitcoinPlus

[Generate Bitcoin](#) | [How Bitcoin Works](#) | [Bitcoin For Websites](#) | [Contact Us](#)

Bitcoin Generation

New: you can generate bitcoin for a friend

Start Generating

Status	Loading
Payout amount	0.0000027 BTC
<div></div>	
Payouts this session	0
View total payouts	
Current speed ?	0
Average speed ?	0
Estimated time per payout	0.00 hours

You must have Java installed to use the bitcoin generator.
If your browser asks you to run the applet, or to install Java, say yes.
Waiting for Java applet to load.

Step 1: Click "Start Generating"
Step 2: Wait while your computer works (leave this page open)
Step 3: Earn bitcoin

It's that easy. Want the explanation? Read [how bitcoin works](#), but click "Start Generating" first so you'll earn bitcoin while you read.

New: The [bitcoin miner for websites](#) is available.

You are not logged in. You can **start generating now** and **your coins will be transferred to your account** when you [sign up](#). If you close your browser your coins may be lost.

For those that want to make money with Bitcoin mining, here are a few considerations:

1. Select the lowest cost electricity state possible. CA is among the highest, and here are a few others at either end:

Lowest-Cost States:

1. Wyoming
2. Idaho
3. Utah
4. Kentucky
5. West Virginia

Highest Cost States:

47. Rhode Island
48. Alaska
49. Connecticut
49. New York
50. Hawaii

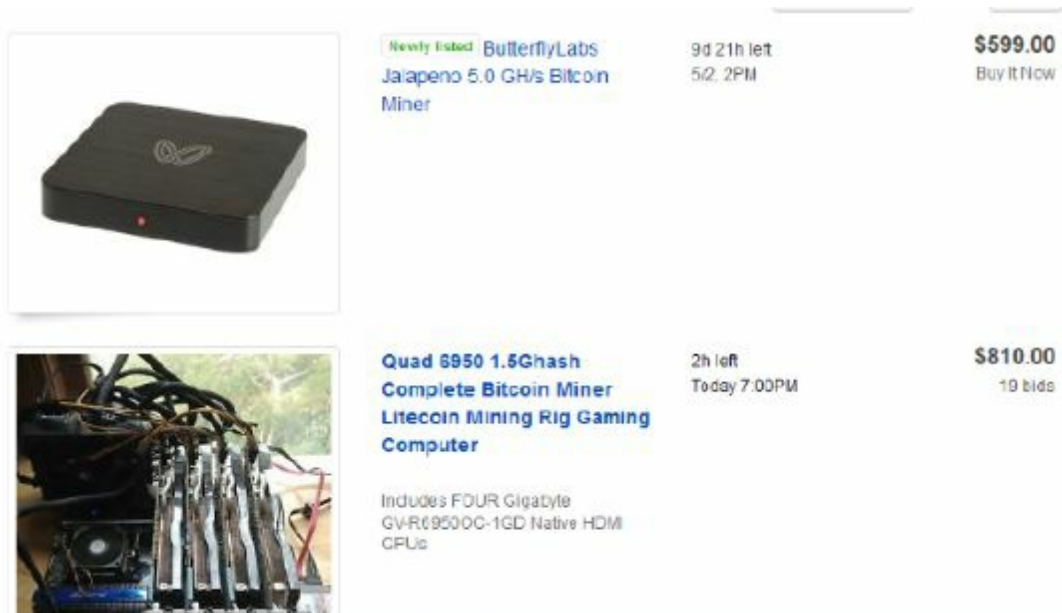
2. If you want to have your own rig (BTC mining server), buy a dedicated one, or build one with an ATI graphics cards. ATI offers the most energy efficient cards with among the fastest hash rates in the low end GPU server world. Now miners are going to ASICS and FPGA's.

Here are a few sources to buy the rigs:

FPGAmining.com

Ebay.com (sample shown below)

Amazon.com for GPU's



We can also buy and assemble our own Bitcoin mining rig. This is similar to building our own computer.

1. We need a power supply. Bigger is better. 500 W + is ideal.
2. We need a motherboard with multiple graphic card slots.
3. We need a mid-range processor of either Intel or AMD brand.
4. We need input output cards to handle extending to other graphics cards.
5. We need multiple graphics cards from ATI. The faster and more memory the better and at the lowest price possible.

How to assemble and get the system working together is beyond the scope of this e-book. One of the better resources is from Scribd at: <http://www.squidoo.com/how-to-build-a-budget-Bitcoin-mining-rig>

Fortunately, building our own mining rig is not the best option for mining Bitcoins. Much like in the real investment world, the best option is buying shares in a mining group. It's almost like buying stock, but without the downside risk and plenty of upside. Still, there are risks.

Problems In Mining Bitcoins

Initially, Bitcoin mining was not very profitable. With BTC/\$ values as low as \$.06 - \$.30, there was not much incentive to mine too actively. As the value of the Bitcoins increased, miners began to make huge margins mining Bitcoins. At the peak, (\$/BTC of about \$260), miners could be making 50 -60 times their investment in the mining rig and electricity. The complexity of the puzzles to solve has increased, as has electricity cost, and the number of miners working to solve the next block, all while the \$/BTC value crashed. These factors have made it so the individual miner does not stand to make much profit from Bitcoin mining unless they invest in serious equipment. Some of the top end Bitcoin mining boxes run over \$10,000.

A better approach for most would-be Bitcoin miners is either to buy into a mining group, or join a mining pool. Mining pools allow individual members to get a smaller piece of the BTC awards given for solving a single block in the chain. Otherwise, an individual miner could be mining for a long time before ever solving the block at the right point to receive their 25 BTC's. Not a wise investment.

We can either build or buy a Bitcoin mining rig as previously described, or join a mining group. We would link our solving power with the rest of the group and split the Bitcoins awarded based on calculations performed.

You can see one of these mining pools here: <https://deepbit.net/>

This area of Bitcoins is ripe for scams, so “buyer beware” applies here.

Potential Bitcoin Disasters, Problems, And Challenges

“Man cannot discover new oceans unless he has the courage to lose sight of the shore.”

Andre Gide

Bitcoin has produced huge positive returns for early adopters - Bitcoin millionaires - and huge losses for those that bought the \$260+ hype bubble in April of 2013. Even the most staunch supporters know Bitcoin has already had multiple stoppages at the site handling 80% of exchanges (mtgox.com), along with hacks of Bitcoin wallets, price crashes from major sellers entering the market, and now government notice of Bitcoin's success. The future will bring more challenges, as this section explains.

Failure Analysis Of The Bitcoin System

Bitcoin relies on a network. The network relies on computers. Internet, telecom, satellite and other communication systems must be free and functional for the computers to form the network. Computers and the network rely on electricity. Any one of these legs of the Bitcoin system can take it down.

Ultimately, Bitcoin relies strictly on the belief that they are rare and worth holding, spending, and transacting with. Unlike gold and silver, there is no use for a Bitcoin and never will be, other than the role as a token residing within a computer network.

Even though there are services now working on creating physical forms of Bitcoins, there is no practical method of confirming the legitimacy of that Bitcoin address and spending power without computing power. Eventually, without electricity and computing power, Bitcoin would cease to exist. This is a critical issue with Bitcoin that will initially prevent wide spread adoption for critical wealth storage.

Some of the physical forms of Bitcoin now afloat are:

<https://www.casascius.com>- offers coins that represent Bitcoins

<http://www.bitbills.com>- offers cards with Bitcoin values on them.

The distributed nature of the Bitcoin network and mining is both a great strength and somewhat of a weakness. The network verifies all the transactions. It also solves any disputed transactions. With a huge and growing number of nodes, there is no single server to hack for the miners, spenders, merchants, or governing body. Without a central storehouse of key data such as a CitiBank, Bank of America, or any number of other major banks, the system is much more robust than almost any other currency system.

Bitcoin has also passed the acceptance test because it has a four-year history. Though major retailers have not adopted Bitcoins, smaller ones have accepted it. Wordpress, Reddit, and many smaller businesses are Bitcoin friendly. There are at least 1,000 stores using Bitpay for merchant services already.

Now that Bitcoin has recovered from the \$260 to \$100 crash and sits comfortably at \$130 today on April 22, 2013, it confers stability to Bitcoin. Time is Bitcoin's friend. There will be fewer options for destroying Bitcoin. Large retailers will no longer be able to ignore it as it continues building credibility and reaches a more predictable exchange value.

Bitcoin is not out of the woods at all. There are dark forces after Bitcoin's hide, and they have already struck. They have a few key targets we will explore next.

Main Targets For Hacks And Attacks

Mtgox.com covers about 80% of the transactions where people buy and sell Bitcoins. It looks a lot like a stock market with price charts, buy/sell orders, and small fees for the transactions. Mtgox.com shut down during the April 2013 crash. They claimed that too many people were signing up for accounts - about 60,000 per day - but that does not seem to be a valid excuse for a shut down that lasted from \$260+ down to around \$100 in BTC exchange value on April 11, 2013.

Bitfloor.com shut down immediately and for good when the crash happened. The exchange function where we trade out of Bitcoins and into dollars, euros, yen, or any other currency or payment system exposes the exchange to significant currency risk. They can lose our Bitcoins and/or our national currency in a blink. This will continue to be an inherent risk in the near future.

Bitcoin blockchain issue - bitcoin deposits temporarily suspended



Mark Karpeles
posted this on Mar 12 09:50

UPDATE 5:25pm JST. We are now resuming Bitcoin Deposits.

<https://support.mtgox.com/entries/21475649--RESOLVED-Outage-57673-B...>

Due to an issue with the Bitcoin blockchain, all bitcoin deposits to MtGox are temporarily suspended.

This will be the case until the Bitcoin issue with the blockchain is resolved.

A brief history of some of the main shut downs:

Mtgox and other Bitcoin exchanges shut down for block chain issues; there are splits in the block chain because of differing claims to be the valid chain. Another similar problem shut down the exchange on June 23, 2012.

The big shut down though, occurred on April 3, 2013 and April 11, 2013. There was no technical difficulty. Instead, Mtgox decided to cool the market instead of allowing it to trade free.

Bitcoin has had several code problems in which there were unverifiable Bitcoins within the network. The first and worst incident occurred shortly after Bitcoin came into existence. In August 2010 over 184 million BTC were generated in a transaction and sent to a few addresses in the network. They were soon spotted as false Bitcoins (BTC), the flaw in the code that created the false BTC was corrected, and within hours the network was back up.

On March 13, 2013 there was a split in the block chain as a result of a large number of blocks created that did not match with previous ones because of a difference in software and the size of the blocks created. This resulted in two sets of block chains depending on the version of the software 0.7 or 0.8 being run. The developers working with Bitcoin.org resolved this split by agreeing to use the 0.7 version and all the transactions checked against that block chain. Even after a 23% drop in Bitcoin value due to this split, Bitcoin bounced back.

The lesson though, is that Bitcoin can have problems with the core code. We all know our computers are not fool proof. Such is the issue with Bitcoin.


Prominent Attacks, Scammers, And Bottlenecks

The cryptographic code for Bitcoin is virtually impossible to crack. That brings all the focus for hackers to use more basic brute force methods of shutting down exchanges and getting Bitcoins. A DDoS is a Distributed-Denial-of-Service attack that sends huge numbers of bot data visitors that overload servers. When an exchange gets hit, inevitably the value of Bitcoins tumbles. This alone would provide enough profit to motivate hackers to crash exchanges for cleaning up the now devalued BTC's. When the exchange gets back up and running, the value of BTC's climb and the hackers have their pay day- possibly. It is also possible that the hackers simply want to crash the service.

InstaWallet was crashed by a similar attack and never recovered.

Other possible attacks:

Government regulations attempt to restrict access to exchanges, label it an investment, or that it is trying to be a currency that threatens the government monopoly. All these fall under Financial Crimes Enforcement Network (FinCEN):



FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities

To provide clarity and regulatory certainty for businesses and individuals engaged in an expanding field of financial activity, the Financial Crimes Enforcement Network (FinCEN) today issued the following guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. The guidance is in response to questions raised by financial institutions, law enforcement, and regulators concerning the regulatory treatment of persons who use convertible virtual currencies or make a business of exchanging, accepting, and transmitting them. Convertible virtual currencies either have an equivalent value in real currency or act as a substitute for real currency. The guidance considers the use of virtual currencies from the perspective of several categories within FinCEN's definition of MSBs.

News Release: http://www.fincen.gov/news_room/nr/pdf/20130318.pdf

Guidance: http://www.fincen.gov/statutes_regs/guidance/pdf/FN-2013-G001.pdf

This black boot agency putting a damper on our monetary freedom is saying:

Users of Bitcoins do not fall under FinCEN rules, but any exchange or wallet services do! They are known as MSB's or money services businesses. This means that any service that transfers, exchanges, stores, or interacts with Bitcoins on a per fee basis, could eventually be the target of the U.S. treasury, FBI, IRS, and any other agency that chooses to participate.

This represents the greatest threat against Bitcoin. Our mystery developers behind Bitcoin saw this attack coming. Their answer was to distribute the ability to exchange Bitcoin. They built in a "black market." What they really built in - was freedom for free people to transact without anyone else knowing about it, taxing it, or being able to stop it.

There is no way short of taking down the Internet and/or power grid for the government to fully stop Bitcoin. That won't necessarily stop them from trying, however.

Profiting With Bitcoins

“Civilization and profit go hand in hand.”

Calvin Coolidge

Successfully trading in any market requires serious study, a keen ability for pattern recognition, and deep knowledge of historical trends and evaluation systems. This section covers the basics of trading only.






Surprisingly, applying basic trading principles often produces the largest profits. More sophisticated trading techniques, sometimes called scalping systems, require more effort and yield small profits, if any at all.





We will proceed from the simple mechanics of buying and selling Bitcoins, to decision criteria for when to buy or sell (the essence of trading), all the way through Bitcoin trading robots or trading services.

Trading Bitcoins

We can buy or sell Bitcoins with anyone who is willing to transact with us. For instance, we could buy Bitcoins locally with localBitcoin.com

Here is a sample screen:

Purchase Bitcoins Online, United States!				
Seller	Payment method	Price/BTC	Limits	
 fy (35, 93%)	Bank: International Wire Transfer	126.49 USD	3000 - 9500 USD	Buy
 BTC Bitabond (0)	Bank transfer United States	129.53 USD	50 - 274 USD	Buy
 BTC joesmo (52, 100%)	Bank transfer United States	140.81 USD	2500 - 17013 USD	Buy
 BTC JimmyBTM (101, 97%)	Cash by mail or Paypal	140.81 USD	50 - 292 USD	Buy
 BTC techcost (2, 100%)	OKPay, Dwolla, Bank Transfer, Western Union	140.81 USD	50 - 151 USD	Buy
Show more >				

Buy Bitcoins with Cash near Atlanta, United States!				
Seller	Distance	Location	Price/BTC	Amount
 Bauhaus (551, 98%)	0.6 miles	ATLANTA, United States	140.81 USD	200 - 10000 USD
 UberNeck (1, 100%)	0.6 miles	Atlanta, Lindridge-Martin Manor, United States	153.81 USD	20 - 250 USD
 Batteryfire (0)	0.6 miles	Atlanta, United States	122.96 USD	25 - 1000 USD
 BTC jroberg (1, 100%)	3.5 miles	Forces De Leon Ave NE@Lakewood Ave N Place Shopping Center, Atlanta, GA 30308, USA, Midtown, United States	256.20 USD	40 - 400 USD

Notice a few interesting and critical developments in this market:

1. Online prices are more consistent, as we would expect.
2. Local prices are both over and under the online price.
3. There is as much as a 24% difference between the lowest and highest prices approximately. Ignore the wild \$256.20/BTC. Everyone else will.

This is key information for day trading scenarios. We could conceivably buy Bitcoins for \$122.96 in lots up to \$1000. Then we could sell them all day long for \$140.81.

Our profit works out to about $8 \times \$17 = \136 (We will neglect gas costs, and buying fractional amounts of Bitcoins)

We could also simply buy Bitcoins online and then sell them locally for a small mark-up. This seems to be the simple trading system of choice for the \$153 and \$147 sellers.

All we need to do is follow the early steps described in the section How to Use Bitcoins. Briefly, we buy Bitcoins using our Dwolla, Coinbase, Blockchain, or other wallet with a custom produced address from a Bitcoin exchange. We can choose MtGox, Bitcoin-24, Bitcoin7, or others.

Then we sign-up for LocalBitcoin. Post our price on their “Sell Bitcoins” section, and we are in the Bitcoin trading business. While this “arbitrage” method of trading can deliver a reasonable profit,

there are bigger profits available for more aggressive profit seekers.

Our best opportunity for trading with Bitcoins involves online only trading. We will buy BTC with our national currency through a trading exchange, and then sell BTC for either our own national currency, or another national currency.

Switching currencies may not be allowed on certain exchanges or in certain countries. Switching currencies between the buy side and sell side of our trade can also add significant complication to our trade. A better move is to stick with one national currency unless we are experienced with FOREX trading already.

Here is what a BTC Buy Order with MtGox looks like for a new account that has not been funded yet:



The screenshot shows the 'Buy bitcoins' interface on the MtGox website. At the top, there are tabs for 'Buy bitcoins' and 'Sell bitcoins'. To the right of the tabs is a fee slider set to 0%, with 0.6% on the left and 0.55% on the right. Below the tabs, there is a checkbox for 'Market Order (buy/sell at market price) This order either gets executed immediately or cancelled.' Below this, it says 'USD in your account: \$0.00000 (add more) | Lowest Ask Price: \$127.99900'. There are three input fields: 'Amount of BTC to BUY' with a placeholder 'Enter amount', 'Price per coin in USD' with the value '127.99901', and 'Total to spend in USD' with the value '0'. A large orange 'BUY BITCOINS' button is at the bottom.

We can enter any amount under “Amount of BTC to BUY” that we have funded. For this new account, that is \$0.00. It could be initially as high as \$4000 for most new accounts. Some exchanges have no limits, and some have staged limits over time.

The “Price per coin in USD” is set automatically here at 127 and change. It will move up or down as we wait to execute the order. This is extremely important to consider. Speed, timing, and execution all affect the price we pay.

After we enter the Amount of BTC to Buy, hit the BUY button, there will be a lag sometimes, but often the order gets executed immediately.

Presto! We are a Bitcoin trader!

Now, for the nuts and bolts of selling Bitcoins, much is the same in terms of fields, with a key difference. When we sell Bitcoins, the exchange takes a slice of the transaction in the form of a reduced selling price. Other exchanges operate differently.

Buy bitcoins Sell bitcoins 0.6% 0% 0.55%

☐ Market Order (buy/sell at market price) This order either gets executed immediately or cancelled.

? Bitcoins in your account: 0 (add more) | Highest Bid Price: \$127.99901

? Amount of BTC to SELL ? Price per coin in USD ? Amount to receive in USD

Enter amount X 127.999 = 0

SELL BITCOINS

The difference between the BTC Buy price and the BTC Sell price is called the “spread.” It is also sometimes known as the Bid/Ask spread. Bid for what buyers are willing to pay, and Ask for what sellers are willing to sell at.

For this case the BUY/SELL is about \$0.40 USD. Not a large spread, amounting to less than 0.5% of the trade.

The good news here is that trading Bitcoins is not administratively expensive. The In/Out costs or round trip are less than 1% of the trade, and often free. Some stock, options, and commodities traders can see In/Out costs between bid/ask, commissions, and exchange fees of closer to 3% or higher. Trading on other Bitcoin exchanges operates in a similar fashion to MtGox.

This is all manual entry trading, not automated or computerized trading. Manual trading can deliver fantastic returns so long as we time our trades and our directions correctly. That is the focus of the next section - answering the question of up or down and when.

General Trading Principles For Bitcoin

Trading technicians focus on three general trends:

First, and most importantly, is the *macro* or *long-term* trend. This is also referred to as a *secular* trend.

Second, is the medium or primary term trend. Third, is the micro, secondary, or short-term trend.

These terms refer to different time periods for different markets, but roughly speaking they break down as follows:

Macro/Secular is for greater than 5 years and usually less than 25 years. Gold and silver were in a secular or macro bull market from 1970's into 1980.

Primary/Medium term trends run for a year or more, but not generally longer than 4 years. The U.S. general stock market as shown by the S&P500 has been in a secondary bull market for several years.

Micro/Secondary trends run less than a year and often refer to moves lasting a few weeks or months. The recent dip in the U.S. stock market is probably a micro bear or down trending market. When it reverses and goes higher, it will confirm that this was a secondary down trend and not a switch to a secular bear market.

All of this seems simple until we have to make the up or down decision. We need only get one decision correct for making a great trade. So, what is the secular or macro trend for Bitcoins relative to our national currency?

The other trends - primary and secondary - are both harder to call and often provide a more limited profit. We will cover how to determine those trends briefly, but first we should look to understand the millionaire maker, a.k.a. the macro or secular trend.

The short answer is: Up. Bitcoin is designed to rise in value on average, every year.

Bitcoin has several forces going for it and increasing the exchange value over the long term:

1. Almost all national currencies are vastly out “printing” Bitcoins. There are about 12 million BTC's as of this writing, while the Federal Reserve creates over \$85 billion in USD's for buying government securities every month.

Simply taking an approximate value for the total U.S. currency in near circulation divided by BTC gives a staggering number of the potential value for \$/BTC.

M2 is a mid range predictor of the currency available for transactions in the U.S. M3 is the broadest but discontinued form, while M1 is more descriptive of cash on hand. M2 sits at about \$10.5 Trillion per Federal Reserve reports.

If only 10% of M2 funds went into BTC, that would be about \$1 Trillion.

This looks like:

$$\text{\$1,000,000,000,000} / 12,000,000 = \text{\$83,333/BTC}$$

Yes, it is extremely unlikely that 10% of M2 will find it's way into BTC. More likely, and currently happening, is that the number of BTC world-wide participants entering the market grows monthly. So, all we really need is 1% of the world-wide M2 value including the active traders in Japan, China, Russia, Europe, and Africa. Bitcoin will soar in value over time, unless either an exchange default, or a government decisively takes it down.

2. Bitcoin is worldwide. Almost 70% of searches for the word Bitcoin come from outside the U.S. Asia drives a lot of the Bitcoin trade; Asia is growing much faster than the U.S. Anything tied to Asian growth, will outperform national centric growth patterns.

3. Increasing taxation and confiscation across the world will drive citizens toward anonymous currencies that have no centralized controlling institution. Many investors in Europe, the U.S, and Asia watched in horror as Cyprus banks and the government stole up to 60% of some bank accounts.

Bitcoin wallets avoid this confiscation threat altogether. There is no bank that can close our Bitcoin accounts or wallets. We can choose to keep our Bitcoins on our computers or USB drives or even memorize them. Bitcoins were designed for just this situation: the need for a private, decentralized, potentially anonymous (hence nontaxable) unit of account, safe from confiscation.

4. More and more stores are accepting Bitcoins. Numbers are hard to come by on the acceptance rate (over 1000 stores), but already there is a core of stores that translate the virtual value of BTC's into hard goods. With that translation, BTC's gain credibility and utility. When BTC's stabilize more over the \$100 point, it will be easier for stores to transition into accepting them.

Wild swings in BTC exchange rates made pricing goods difficult for merchants. Also, with a limited stock of BTC's circulating, there is not enough demand as the user base is limited. When bitcents are traded and even microbits and lower denominations are more common, then the distribution of BTC's can spread. Wider distribution will mean more customers with BTC's to spend, leading to stores meeting the demand.

Already nightclubs such as EVR in New York City accept Bitcoins with a phone app. Trend setting merchants such as this will bring Bitcoin all the popularity needed to close the gap with traditional, centralized currencies.

5. No significant competitor can challenge Bitcoins entrenched user base, which has been developed over 4 years. Already the Bitcoin competitors are gathering funding and moving in to take over. They will have trouble succeeding because their benefits are marginal, and they will have to build a new user base. We will discuss the future of Bitcoin and possible competitors in a later section.

All the above factors will send the general trend for Bitcoins relative to national currencies steeply upwards. This trend will continue for many years, possibly as far as 20 years, until there are conflicts within the currency system.

We can then buy the long-term trend and sit tight while our wealth increases, when comparing BTC to our national currencies.

For primary and secondary trends, the simplest trading methodology is also one of the most effective.

The chart below (found on <http://www.Bitcoincharts.com>) shows a 4-month price window of closing prices, with exponential moving averages from 10 and 25 days and the purple or shaded portion represents Bollinger bands:



What we are looking for are extreme moves where the short-term trend moves significantly beyond the longer-term trend. This tells us that a bubble or reversal may be at hand. A perfect example occurred during the April 1-11 time frame. The chart shows with the Bollinger bands, and the two exponential moving averages shown by the brown and purple lines (the 10 day is almost always above the 25 day EMA line for those with black and white readers), where the danger zone happened. All experienced traders knew there was a steep collapse dead ahead.

At the Financial Survival Center (<http://www.financialsurvivalcenter.com>) and [@financialsurvyl](https://twitter.com/financialsurvyl) twitter feeds, there were warnings saying to sell out of BTC immediately. When the price leaps outside of the upper bounds of Bollinger bands, and the short term EMA moves much higher than the long term EMA - jump off the BTC ride into a national currency.

Conversely, when the BTC value dives deep into the Bollinger bands, and the short term EMA crosses below the long term EMA line, there is a good opportunity to buy shortly. Then we can ride

the short term EMA back up as it re-crosses above the long term EMA.

The main reason we can make these trades confidently is that there is a fixed amount of BTC's in the system. That gives it a strong upward trend bias. We also know that when there is too high of a price spike, the down move will be swift and relatively short-lived. All of this knowledge stems from our most important call – in which Bitcoin is in a secular bull market against all national currencies.

This is all manual trading. More automated trading uses key techniques such as:

- Stop Loss orders (for selling based on a triggered loss level)
- Stop Age (time based selling)
- Target Price (buying or selling based on reaching a price)
- Buy Order Protection (forces over priced orders to below current market rate)

The stop loss and target price tools are the most critical. With a high beta market, the stop loss should be set as high as 20% or even 25%. Lower beta markets can use a 10% stop loss, or what is known as a tight stop loss. This translates to buying in at \$100 and setting a stop loss at about \$80.

While there could be much more written for covering other trading techniques, this basic knowledge will suffice. We can spot the too highs and too lows for selling and for buying. That is all we need to do for making a handy profit with Bitcoins.

For those interested in learning more about trading any currency or market, the challenge is there are *too* many books or courses available. [**Financial Survival Center**](#) has a free newsletter for trading, general investing, alternate income, and alternate currency investing.

Bitcoin Application Development

The trend for Bitcoin trading leads toward trading robots. While we might consider this a threat, it can be the saving force for Bitcoin. Bitcoin suffers from high volatility or Beta as explained earlier. Trading robots can reduce this volatility. Trading robots, or software, that tie into trading exchanges via Application Development (Programming) Interfaces, will make frequent small trades when there is movement in the market either up or down.

These frequent trades for small gains (and losses), are called scalping trades. They steady the market considerably because price movements immediately result in buys or sells against the move.

Mtgox.com has automated trade platform API's with two forms:

- HTTP API
- Streaming websocket API

All relevant trade information can be accessed through these protocols for trading.

There have been a few free trading bots written in PHP, but they were pulled off sites quickly. A robot that is consistently profitable is worth a fortune. The essence of what makes the robot work is being able to spot the price trends instantly, execute instantly, and avoid significant losses.

There are downsides for trading software robots. They can crash a market when they gain too large a market share. This is partly what happened in the famous Oct 1987 Black Monday crash. Mutual funds triggered excessive selling with computerized trading platforms.

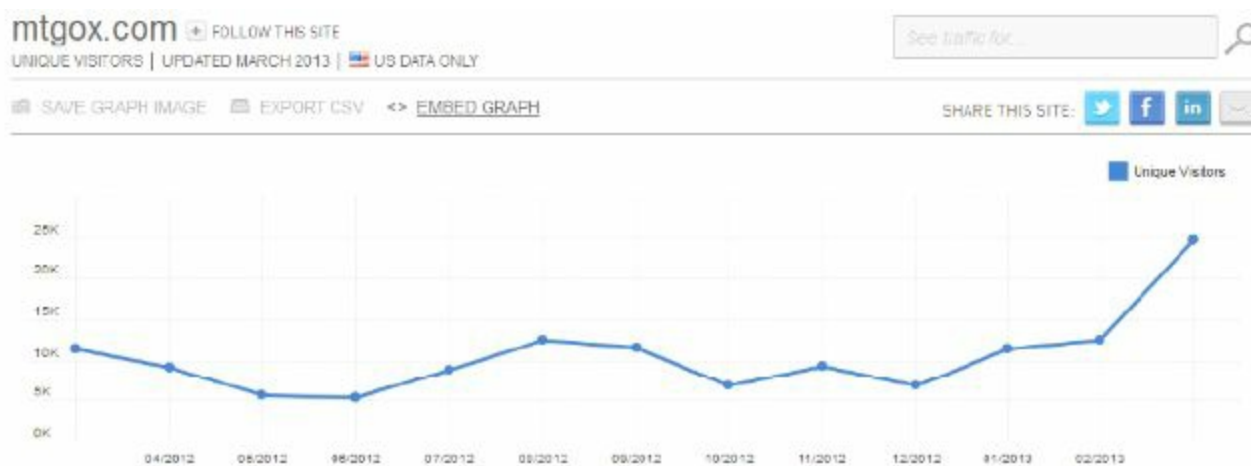
Future Of Bitcoin And Alternative Currencies

“He who refuses to embrace a unique opportunity loses the prize as surely as if he had failed.”

William James

Opportunities And Dangers Ahead

Here is MtGox.com's traffic estimation chart for only U.S. web access:



Going from 5k unique visitors per month (UV) to over 25k UV shows that the future looks bright indeed for both Bitcoin and mtgox. We would see even greater growth from international web access graphs. The majority of Bitcoin users are coming on board from outside the U.S.

Opportunities being seized and presented to the market place include:

1. Physical forms for Bitcoins with bitbills, Cassascius, and others.
2. A myriad of applications for Android, iPhone, iPad, Windows, and the tech favorite, Linux. aCurrency, an Andorid app for currency conversion now links to Bitcoins. Bitcoin Wallet for Android and many others allow Bitcoins to be used almost like a credit or debit card, from our phone. Either we scan in our Bitcoin address and wallet information from a generated QR code, beam it, email it, or go through a web interface (plus other types of withdrawals not yet fully functional).
3. Merchant services from bitpay, OkPay, MtGox, Dwolla, etc. are making it easier for merchants to accept and cash out their BTC's.
4. Trading platforms are springing up to relieve Mtgox of its dominant role. Mtgox is not universally approved of because it has stopped trading at the most critical points, and often has lower prices.
5. There are also a host of competitors on the horizon. Ripple is the biggest and best financed so far.

Produced by a company called OpenCoin Inc., Ripple is based on similar concepts to Bitcoin. Ripple is open source and distributed around a network exactly like Bitcoin. One of the key differences is that there are already about 100 billion ripples in existence, but they are fed into the system on a controlled basis.

It also uses something called social capital for backing financial capital. Plus, it has trust features for selecting networks to use for payments or transfers. What has the Bitcoin world suspicious though, is that OpenCoin Inc. is backed by large Wall Street venture capital firms.

Ripple has betamax stamped all over it. Bitcoin is working, out of the gate sooner, belongs completely to a voluntary community, and is not affiliated with Wall Street interests.

Other digital only competitors include Litecoin, Lucre, OpenMoney, OpenCoinage, Voucher-Safe, and many more.

Entrenched competitors that are not seeing the growth, but do have tangible assets - gold and silver - backing them include:

- Pecunix
- GoldMoney
- BullionVault
- PerfectMoney
- LibertyReserve
- Tecnocash
- C-gold
- Formerly available e-gold
- Global Digital Pay

These gold or silver backed currencies are not widely used, traded, or accepted. They do have the advantage of being backed and convertible into physical precious metals. Without wide market acceptance, however, their future is limited.

6. Most critically, there are efforts for backing Bitcoins with gold or silver. This is a critical step that will cement BTC's as a functional form of money. There are reasons for not taking this step, as it decentralizes the network if there must be storage for the gold. However, a de facto backing by gold would mean that the value of a BTC is respected enough that it can be tendered for gold.

Agents For And Against Bitcoins; Alternative Currencies

Governments, banks, the Federal Reserve (and all central banks), Visa, MasterCard, American Express, taxing agencies, some tech companies such as Apple, Microsoft, Google, Amazon, and the United Nations are all staunchly opposed to Bitcoin.

In time, Bitcoin can put many a bank under. No more credit card fees, bank accounts fees, or controlled interest rate schemes can flourish when we can provide our own banking services through choice.

On the plus side, the Internet software groups support Bitcoin strongly. The younger generation has adopted it as their own. Asia is betting on Bitcoin to preserve their hopes for increasing wealth while their central banks create massive inflation. Those wishing to keep funds from being confiscated will use Bitcoin (as the Cyprus event demonstrated).

Forces allied with Bitcoin are more widespread, determined, active, and clever than those opposed to Bitcoin. Bitcoin seems to be emerging victorious.

Predicting Prices For Bitcoins

Already, we've calculated a possible worth for \$/BTC north of \$80,000.00 based on the U.S. M2 value.

Including all the worlds' currencies in that calculation will send that number up by 4 fold or more.

More important than the currency value of a BTC, is what the realizable value of one will be. We could, and probably will, have a currency regime change between now and 2139 when the last Bitcoins are mined. The question is what will we be able to buy with a Bitcoin, or a dollar for that matter?

The U.S. dollar will buy less of the critical goods over time, as has been the case ever since 1929. The value of a dollar has declined roughly 97% over that period. Bitcoins will move higher and lower, but will not experience a waterfall decline - unless attacked and stopped by governments or banks. Bitcoins will continue their market penetration, pushing aside inflated national currencies.

Expansion Markets For Bitcoins

There are many opportunities for Bitcoin entrepreneurs.

1. Bitcoin consulting for getting online and offline merchants integrated with Bitcoin appliances, pricing, out-conversion, marketing, and trading.
2. Developing and selling Bitcoin trading robots. This is a huge potential opportunity for those with the software skills for tackling the coding along with the trading chops for making the robot a profit winner.
3. Bitcoin financial transfer agents for converting from debit cards, credit cards, loans, gold, silver, local currencies, creating transfers, etc. The old guard institutions consider Bitcoin the enemy. This leaves an open window for those willing to get over the MSB hurdles.
4. Bitcoin network monitoring codes for alerting Bitcoin users of unusual activity across the network. This would be similar to the stock market where futures indicate the direction of the market before it opens. With this service, Bitcoin users could be alerted to when there is a market rocking event and make decisions accordingly.
5. Bitcoin advertising network. One of the biggest issues for Bitcoin is that businesses cannot easily use it for buying business services. An advertising network suited for Bitcoin clients will absorb the Bitcoin flow from online merchants. Google refuses to convert to Bitcoin, so another avenue is needed.

Bitcoin seems to be here to stay. Frequent updates for trading and Bitcoin events can be found at:

<http://www.financialsurvivalcenter.com>

Sign up for the newsletter and follow [@financialsurvvl](#) on Twitter for frequent trading tips, risk warning, and investment strategies about Bitcoin and alternative investments.

One of the most active forums for Bitcoin: <https://bitcointalk.org>

To a future of Bitcoins...and freedom.

Your Bitcoin Guides,

Mark D. Solomon & Daniel Forrester

One Last Thing...

Was this book helpful? Did you hate it?

Was it worth your time?

Whether you loved it, or found it useless, your opinion is valued highly by us, the Amazon Marketplace, and most importantly – **fellow readers**.

Please click [here to leave a review](#) about this book – it will only take a minute.

Thanks!

Appendix A - Major Bitcoin Developments & Timeline

1990 - David Chaum founds DigiCash Inc. Transactions were unique based on cryptographic properties, similar to Bitcoin.

1998 - DigiCash, Inc. files bankruptcy, and is sold to Ecash.

2002 - InfoSpace buys Ecash.

2008 - Satoshi Nakamoto makes hundreds of posts to cryptography forum metzdowd.com. He publishes a research paper detailing a Bitcoin concept.

8/15/2008 - Patent #20100042841 filed for a Distributed Encryption Key Invention

8/18/2008 - Bitcoin.org domain reserved out of Helsinki, Finland.

2009 - Bitcoin network forms with the open source client and first bitcoins issued.

2010 - Mt.Gox bitcoin exchange formed.

2011-2012 WikiLeaks, Wordpress, Reddit and small online merchants accept Bitcoin. Bitpay reports over 1000 merchants using their service.

Bitcoins have a major crash from \$30 to \$2 in late 2011.

Coinbase sells over \$1 million BTC in a single month.

2013 - A split occurs in the Bitcoin transaction log or block chain. It is eventually resolved.

FinCEN - The financial crimes are of the U.S. Treasury puts Bitcoin exchanges on notice that they are considered under their rules.

Mt.Gox, the major Bitcoin exchange, shuts down during a crash from \$266 to \$105.00.

Appendix B - List Of Main Bitcoin Services And Websites

Bitpay is the leading merchant processing service and has the largest customer list for stores accepting Bitcoin.

This list was current as of April 2013 – Please note that many of these sites/stores may no longer be operating or accepting Bitcoin.

Source: <https://www.spendbitcoins.com/places/>

- [**ModifiedController.com**](#) - Modified Xbox controllers.
- [**Alpaca Products for Bitcoins**](#) - Alpaca socks.
- [**Babbletees**](#) - Design Savvy Science/Academic Based T-Shirts. Bitcoin accepted at checkout.
- [**Heatslingers.com**](#) - 100% Authentic Nike Dunk SB, Air Force 1's, Air Jordans and Clothing. Accepts Bitcoin.
- [**R-Shirt**](#) - Accepts Bitcoins for geeky pirate R-Shirts.
- [**Pirates of Savannah**](#) - Website for historical adventure novel - ebooks and audio books for sale.
- [**Video Seconds**](#) - New DVD concerts, movies, select CD's and misc eclectic products. Ships International.
- [**Happy Tree Cosmetics**](#) - Natural hand made cosmetics. Bitcoins are accepted on the main business page for gifts.
- [**ottonormalo**](#) - we offer premium postcard, audio books and outstanding photography (German website).
- [**VPN Service by Private Internet Access**](#) - Private Internet Access is the leading VPN tunnel service provider.
- [**cryptoanarchy.com**](#) - We sell embroidered polo shirts, bumper stickers, magnets and some computer components.
- [**CRON-O-Meter**](#) - CRON-O-Meter is a premium web application for tracking your nutrition and health data.
- [**Bitmit**](#) - Biggest Bitcoin user to user shopping marketplace (auction house and buy now).
- [**FUSA**](#) - FUSA offers dedicated servers, virtual private servers and colocation services.
- [**BTCInstant.com**](#) - We provide instant Virtual Master Cards (purchased with Bitcoins) sent to your email.
- [**txt4coins.net**](#) - Worldwide SMS service. No registration, pay-per-use, bulk messages supported, full API.
- [**NESTORGAMES**](#) - NESTORGAMES manufactures and sells physical board games worldwide in a nice portable package.
- [**Shire Silver**](#) - Shire Silver makes physical precious metal easy to trade and handle.
- [**Stomp Romp Guitars**](#) - Stomp Romp is a pedal-centric guitar store in New Hampshire, USA. We ship worldwide.
- [**Anonymous Ads**](#) - Unusual and transparent advertising network that doesn't collect personal data about users.
- [**Stateless Sweets**](#) - Delectable homemade, all real ingredient candy, delivered to your home as a treat.

- [**BitLasers**](#) - We sell handheld lasers and accessories for Bitcoin.
- [**George's Famous Baklava**](#) - George's Famous Baklava has been baking and shipping baklava online since 2009.
- [**Coinabul**](#) - The first Gold to Bitcoin marketplace. We sell gold and silver for Bitcoin
- [**Bits For Coins**](#) - Quality Dedicated Servers, VPS, VPNs and seedboxes.
- [**HowToTeachEnglishOnline.com**](#) - Discover how to teach English online and make money. The e-book will show you how to
- [**ClintonCharlie**](#) - Designer Jeans label - Now accepting BTC payment!
- [**MindTag Tecnical Support**](#) - MindTag is a web development company that is built to grow your business online.
- [**Escape To Life**](#) - Private Swiss detox clinic. Rapid, gentle and discreet 5-day escape from painkillers.
- [**BitcoinAg**](#) - Purchase silver from BitcoinAg and receive it straight to your door within 5 business days.
- [**Dashing Valet Dry Cleaning**](#) - Dry cleaning delivery service.
- [**Guerilla Packs**](#) - Versatile backpacks.
- [**Eastern Mountain Sports**](#)
- [**Private Internet Access™**](#) - Private Internet Access™ is the internet's leading VPN service provider.
- [**Minethings.com**](#) - Minethings.com is a fun online game that pits you against people around the world.
- [**Volternal Consulting**](#) - Volternal Consulting is an IT Consulting firm that specializes in using Free, Libre,
- [**Agorist Marketplace -- flags us as having malware when this link is active**](#) - Connecting the Free Market Community since 2012.
- [**Real G&G**](#) - Here you can convert Bitcoins to what ever you like.
- [**fiveminutecoin**](#) - Get free Bitcoins or advertise cheap with the instant advertising feature.
- [**Bitcoin Magazine**](#) - Bitcoin Magazine is an international distributed print publication covering all things Bitcoin.
- [**Vaper's Mark**](#) - Vaper's Mark is an electronic cigarette company that makes premium e-liquid and wooden cigarettes.
- [**BitJack21**](#) - Bitcoin blackjack
- [**BitcoinAdvertisers.com**](#) - Advertise for Bitcoins
- [**BitcoinNetworks.com**](#) - Bitcoin hosting and cloud
- [**Bitronic Technologies**](#) - Bitronic Technologies now accepts Bitcoins as a payment method.
- [**Bitronic Technologies Web Hosting**](#) - Bitronic Technologies accepts Bitcoins as a payment method.
- [**XSNL.NET Internet Services**](#) - Get your own webhosting for Bitcoins.
- [**honestbeef**](#) - Selling Australian grass feed beef direct from the farmer. Transparent pricing.
- [**MyDogtag.com**](#) - Design and order your own custom Dog Tags with the online Dogtag Generator! Pay with Bitcoins!
- [**Qiqqa**](#) - Qiqqa is free research management software. You can purchase Premium membership using Bitcoins.
- [**North Outboards**](#) - We mainly sell used boat parts. We will accept Bitcoins

- [**SuperSeedbox.co.uk**](http://SuperSeedbox.co.uk) - Seedbox and dedicated server provider.
- [**Mach 1 Web Design**](#) – Create your own website, or let us create one for you.
- [**CISTHENE**](#) - "Jewelry is personal."
- [**DOTS Investment Strategy**](#) - This simple "Sell in May and Go Away" investment strategy outperformed the S&P500.
- [**BitcoinAdSmart**](#) - BitcoinAdSmart offers the most fully intuitive Bitcoin advertising service available.
- [**Schuhwelt.com**](#) - Sale of brand name shoes like Birkenstock, Meindl and other german top brands.
- [**Seals With Clubs**](#) - Seals With Clubs is Bitcoin poker. We have ring games and tournaments.
- [**FastCash4Bitcoins**](#) - We are a direct buyer of Bitcoins and offer fast payouts.
- [**Pacific Bliss Massage**](#) - Pacific Bliss Massage is Vancouver's most blissful massage and integrated healing center.
- [**Microtronix**](#) - Webhosting, Vserver, Domains, etc.
- [**Ferroh**](#) - Trade Bitcoins for Diablo 3 gold!
- [**BeeVPN**](#) - Privacy and Protection done right!
- [**Bithosting.info**](#) - Web hosting from 0.5 BTC/month or \$5/BTC/year!
- [**Bam+Boo Baby**](#) - Bam+Boo Baby Products offers a range of reusable cloth diapers and other eco baby items.
- [**mumble4bitcoin**](#) - Exclusively for Bitcoin: mumble-server slots at an unbeatable low price.
- [**Morgan Digital Engineering Services**](#) - It's been said that everyone on earth has at least one "Million-Dollar" idea in their lifetime.
- [**YogiWay.eu**](#) - European yoga eShop - yoga mats and yoga tools
- [**SurvivalFood.com**](#) - SurvivalFood.com is a retailer and wholesaler / consultant of emergency and survival items.
- [**Straight Talk**](#) - MVNO of AT&T Mobility Prepaid cell phone service.
- [**Bitcoin Bundles**](#) - Bid on bundles of Bitcoins and occasional special auctions.
- [**OZBTC**](#) - australian Bitcoin classified
- [**anti-interception**](#) - anti interception stealth phones , privacy protection tools
- [**Pixel Punch Design**](#) - Pixel Punch is a web and graphic design company. Based in the UK; accept international payments.
- [**Quantum Kiwi**](#) - Quantum Kiwi - Web & I.T Solutions We provide Premium CLOUD Web Hosting services.
- [**Webvox**](#) - Web design and web programming.
- [**Copa Apartments**](#) - Short-term apartment rentals in Rio de Janeiro, Brazil!
- [**WASDhost**](#) - Extremely cheap Minecraft hosting, Try our one gigabyte of RAM server to test it out.
- [**GarageFarm.NET**](#) - GarageFarm.NET is a small but powerful internet farm.
- [**Bluetreehost**](#) - Bitcoin web hosting from an established web hosting company with a solid track record.
- [**All Things Luxury**](#) - Jewelry for less. Up to 75% off retail prices, plus free shipping. Vast selection of jewelry.
- [**Diplomat Limited**](#) - We supply software and hardware to the taxi and private hire market.
- [**YOKU Cloud Hosting And VPS Servers**](#) - Since 2001 Yoku's team has specialized in VPS

Servers and Cloud Server Hosting.

- [**PhoneSomeone**](#) - Telephone wholesaler of second hand equipment.
- [**TSHIRT LAB**](#) - T-shirts and Blotter Art - designs inspired by all manner of coolness!
- [**Btcgriffin- Bitcoin Lottery**](#) - Play Lottery with Bitcoin
- [**Bitwein**](#) - Buy high quality wine from palatinate for Bitcoins.
- [**darkFunction Software**](#) - darkFunction Editor is a 2D sprite and animation studio for game developers.
- [**Fiber Back Up Canada Inc**](#) - IT company. We fix computers and stuff.
- [**Adamant Barbell**](#) - Home and commercial fitness equipment.
- [**Lighthouse**](#) - Flashlights, batteries, chargers, outdoor gear, etc.
- [**Directbizware**](#) - Home and Business software for Bitcoins
- [**Bitwein.de.vu**](#) - Wine for Bitcoins
- [**VisualCity**](#) - SEO, Web Design, Adwords Management, Internet marketing.
- [**Cups and Cakes Bakery**](#) - The first business to sell cupcakes for Bitcoins.
- [**BTC-Trader a MtGox trading client for windows**](#) - BTC-Trader is a MtGox Bitcoin trading client for windows. Compared to MtGox ' web int
- [**Ico6**](#) - Do you have enthusiasm for Computers? Gaming? Science?
- [**CoinUploads**](#) - File storage and sharing for Bitcoin.
- [**Health Kismet**](#) - Health Kismet makes Incredible Greens, a green superfood supplement.
- [**Bitquestion**](#) - Get expert help with Bitcoins: ask away your hard questions!
- [**CleverPuffin.com**](#) - A UK based web host which exclusively accepts BitCoin for payment.
- [**Torfl**](#) - Torfl Bitcoin Raffles
- [**House of Smoke**](#) - Tobacco shop with glass pipes and waterpipes. Bulk bags of tobacco.
- [**SuperSeedbox.co.uk**](#) - SuperSeedbox.co.uk offers high speed, 100% anonymous seedboxes and servers.
- [**FireSteel.com**](#) - Firesteel fire-making rods used by the military, hikers, hunters, and survivalists.
- [**Mono für Alle!**](#) - TShirts made in Berlin from garbage.
- [**Keystone Pet Place**](#) - Since 2007 Keystone Pet Place has been offering a wide selection of pet food and supplies.
- [**Primo Maggio**](#) - Original Italian food at its best. Gotta love the homemade antipasti, pasta, and desserts.
- [**Fabelhaft Bar**](#) - Floor and Bram are making some of the best cocktails you can find in Berlin.
- [**Vinyl Living Room Longplayer**](#) - Nadim has an unbelievable selection of rare and hard-to-find vinyl records to offer.
- [**room77**](#) - The restaurant at the end of capitalism - or so some call it. :D Best burger!
- [**37SOLUTIONS**](#) - 37SOLUTIONS, LLC resells Rackspace Cloud Sites to make the cloud affordable.
- [**BioStim Pty Ltd**](#) - We are a Australian agriculture fertilizer and food company that is now accepting Bitcoins.
- [**Gadgets Direct**](#) - Australia's largest gadget site with over 18,000 gadgets all with free shipping.
- [**Verita Creative**](#) - Very Tasteful Business
- [**Vintage Lighters**](#)
- [**Giftsforcoins.com**](#) - This is a gift store selling various gifts in ONLY Bitcoins!

- [**Royal Bitcoin**](#) - Bitcoin dice game, no sign-up or registration required. Offers a 1% rakespace and affiliate commission.
- [**SimpleVPN**](#) - Premier VPN service provider with servers in 19 countries and world class customer service.
- [**Lucky Hasher**](#) - Online Raffles for Bitcoins and Bitcoin Mining Hardware.
- [**Chromaitccreative**](#) - Post interactive advertisement starting from 0.0001 BTC per valid answer from the read
- [**Jardim Sonoro \(Sound Garden\)**](#) - Music and Sound Producer Music Branding Sound FX Composer.
- [**Hong Kong Massage**](#) - Massage Outcall service for hotels in Hong Kong.
- [**GigaTux**](#) - VPS and web hosting business offering services in the UK, USA and Germany. Accepts Bitcoins.
- [**HOTServers LLC**](#) - Specializes in DoS and DDoS attack protection and mitigation.
- [**Qroo Power Sports**](#) - Qroo power sports is all about fun through exercise.
- [**XMLGold.eu**](#) - XMLGold is an exchange provider between digital and e currencies.
- [**Massage By Lexxie**](#) - Esalen, Deep Tissue, & Reliki Massage for men, women, & couples.
- [**Agriturismo Il Falcone**](#) - In the quiet countryside of Sedena di Lonato (9 km from Desenzano del Garda – Italy).
- [**Kiwi Bird Kollektable Koins**](#) - Kiwi Bird sells numismatics (kollektable koins), bullion, banknotes, exnumia, etc.
- [**Grippit UK Ltd**](#) - Signage and Display Board Manufacturers - specializes in bespoke aluminum displays.
- [**Sprung Bags**](#) - Ice Water Extraction Bags - herbal resin extraction.
- [**Amagi Metals**](#) - Amagi Metals is a global eCommerce precious and base metal dealer located in Denver.
- [**Personal Online Tutor**](#) - Personal Online Tutor is an online tutoring company for learning computer graphic and design.
- [**Maplewood Boot Camps**](#) - We offer fitness services such as personal training and group boot camp sessions.
- [**MMOclub**](#) - • buy World of Warcraft account, FFXI accounts, Runescape accounts, etc.
- [**PNTHR.com**](#) - Web Design and App Development firm based out of Boston, MA.
- [**finetunes.net**](#) - Finest mp3s for you.
- [**Dazzlepod**](#) - Large password list for use in penetration testing and security audit.
- [**Discfree Arcade Rentals**](#) - We rent out full size classic arcade games to the San Francisco Bay Area.
- [**Robertson Robots**](#) - Electromechanical design and fabrication, programming, and prototyping.
- [**Bigpond Movie**](#) - Bigpond gift voucher codes used to buy bigpond movies.
- [**ChicagoAnimation.com**](#) - Flash animation web site design, internet marketing and social media marketing services.
- [**Firehouse BBQ**](#) - Cajun & Creole Restaurant · Barbecue Restaurant 2100 South 565 East, Salt Lake City.
- [**XPI LLC**](#) - We sell, gun accessories, paracord, camping, and outdoor / survival gear.
- [**Card25.com**](#) - Print shop that accepts Bitcoin for full payment.
- [**iIMAGE46**](#) - Unique Personalized Art

- [**River Mountain Mfg**](#) - Lodge and Western furniture and furnishings Mfg.
- [**Namworld**](#) - Web Hosting - Web Design - Domain Registration - SLL Certificates – Printing.
- [**Green Payment Processing**](#) - Merchant Processing in the United States.
- [**VPNme**](#) - A VPN service provider that takes your anonymity, privacy and security very seriously.
- [**Gifts4Coins**](#)
- [**BTC Bunker**](#) - We sell outdoor gear, gun parts, clothing, and survival gear.
- [**Michad Computer Consulting**](#) - Michad Computer Consulting is a small town, do it all firm.
- [**True Art Gallery**](#) - Elizabeth Elkin is a renowned professional artist with an international reputation.
- [**vandemous**](#) - Selling tech support for computer choices in the 2013 and beyond.
- [**UnixStickers**](#) - Linux and Open source stickers to customize your Notebook and PC!
- [**Tumult Inc.**](#) - Using Tumult Hype, you can create beautiful HTML5 web content.
- [**YourSeedbox**](#) - We offer Dedicated and Shared seedboxes with 100Mbit+ connections in the CLOUD.
- [**GoGreenSolar.com**](#) - GoGreenSolar.com is a value added supplier of green energy products and services.
- [**DR Grove Software LLC**](#) - Website Design, Development, Software Development, and Web Hosting.
- [**Atlanta Kick Karate and Kickboxing**](#) - Largest Martial Arts School in Atlanta teaching kids and adults for the past 16 years.
- [**BTC Toys**](#) - We are the leading online adult product retailer that sells exclusively to the Bitcoin community.
- [**K & S Trading LLC**](#) - We sell discounted surplus parts used in the repair and maintenance.
- [**The Fairy Wing Repair Shop**](#) - Retailer of enchanting gifts and curiosities. Bitcoins taken both online and in store.
- [**OzHobbies**](#) – Online shop for LED Throwies, robot and electronic kits.
- [**Crizzle's Buttons**](#) - I make custom & alternative pin-back buttons!
- [**Turismo Supremo**](#) - We are a Tour Operator from Venezuela.
- [**Vapetropolis**](#) - We sell specialize in the sale of Portable Vaporizers for herbal use.
- [**BitElectronics**](#) - Buy consumer electronics using Bitcoin. Free shipping to EU!
- [**Witch Trials, Legends, and Lore of Maryland**](#) - A book about witch trials in the state of Maryland.
- [**MonsterMegs Web Hosting**](#) - MonsterMegs provides hosting solutions for small businesses, individuals, and enterprises.
- [**Dynasty Systems**](#) - Dynasty Systems is a server, storage and workstation source with extensive support.
- [**Pirate Cove**](#) - Drops-shipping and wholesale of sunglasses, handbags, shoes, and more. Bitcoin proudly accepted.
- [**Liberty Crier**](#) - Liberty Crier is a news outlet that provides breaking news and analysis/
- [**Open Source Powered**](#) - 3D Printer filament and supply company who also does local work rapid prototyping.
- [**Rife Digital Stores**](#) - Rife Digital International, are the worlds largest suppliers of Rife Machines.

- [**Soccer Shirts Online**](#) - Soccer shirts online offers a wide range of soccer uniforms, including soccer shirts and apparel.
- [**7 Buck Tees**](#) - 7 buck tees sells politically incorrect T-shirts for \$7. We accept Bitcoins.
- [**Scry Anti-Theft Software**](#) - Scry Anti-Theft For Mac. Track your stolen Mac. Protect your identity. Keep your data.
- [**37SOLUTIONS**](#) - We resell premium Rackspace Cloud Sites web hosting at a mom & pop price.
- [**The Bitcoin Store**](#) - It's arguably the biggest store that sells over 500,000 electronics items exclusively.
- [**Bitherbs.com**](#) - We offer here natural herbal products belonging to or related to Traditional Chinese Herbs.
- [**VertVPS**](#) - VPS Servers - KVM and OpenVZ Virtualization, Full root access, North America and France.
- [**LGCards**](#) - Instant delivery of your favorite game cards, such as Xbox Live and Playstation.
- [**Hosterbox**](#) - Hosterbox is a Canadian based company operating in more than 170 countries around the World.
- [**AltusHost Inc.**](#) - AltusHost has been providing quality Web Hosting services since 2008.
- [**Retrotowers**](#) - We sell retro game controllers, cables, flash carts and clones.
- [**Bitmit - Electronic Project Parts From 99p**](#) - Low price electronic project parts.
- [**Spanish Highs Mountain Guides**](#) - Spanish Highs Mountain Guides provide a wide range of activity holidays.
- [**Rollingdale Winery**](#) - Rollingdale Winery is a small 100% family owned winery located in West Kelowna, BC.
- [**Digifuzz**](#) - Hand crafted and calibrated active monitor loudspeakers.
- [**Litehosting.org**](#) - Litehosting is a VPS provider which accepts BTC, LTC, NMC, RUC, and NVC.
- [**FeedPies**](#) - FeedPies : An Online Rss Feed Reader Script.
- [**Koch Architecture LLC**](#) - Architecture Firm
- [**Soft Shop**](#) - We have the best software at the lowest prices!
- [**AJ Processing**](#) - AJ Processing offers Podcast Transcription, Typing, Data Entry, Scanning, & Research.
- [**OrangeWebsite.com - Anonymous Web Hosting**](#) - OrangeWebsite.com offers affordable ICELAND based hosting and domain solutions.
- [**AKG Guitar Lessons**](#) - AKG Guitar Lessons provides you with high quality guitar lessons in the comfort and convenience of your home.
- [**BasicBitcoin**](#) - The business sells a book about Bitcoin.
- [**GoMatkot**](#) - GoMatkot Offers Israeli beach paddles, or rackets.
- [**Grapholab Communication**](#) - Who are we? A group of naive who never says no. The union of many talents.
- [**Tespia Host**](#) - Tespia Host is a VPS and Server hosting company. They also offer Cloud Backup services.
- [**Bitcoin Video Casino**](#) - Play casino games with Bitcoins. No registration needed, and you can start playing in minutes.
- [**SovereignLife**](#) - SovereignLife is a membership-based service offering a wide range of

information.

- [**Ethos Healthy**](#) - Ethos supply a unique and exciting array of cutting edge health products for health.
- [**nexus osx86**](#) - computers , gadgets , geek clothes , Bitcoin and more.
- [**puroexpress**](#) - Online cigar shop accepting Bitcoins.
- [**cdkey-hut**](#) - CDKey-Hut is the best place to purchase digital codes online.
- [**Patcht**](#) - We are online custom clothing brand based in Sydney Australia. Choose your design!
- [**Krager Custom Wood Products**](#) - Woodworker. I make heirloom quality items to your order.
- [**Aspire Auctions**](#) - Online Auctioneers of Art, Antiques and Jewelry
- [**SuperSeedbox.co.uk**](#) - Dedicated servers and high speed torrent seedboxes. 100Mbs and 1Gbs servers and slots.
- [**RummageiT**](#) - Selling new and used items, including computers, laptops, tablets Monitors and accessories.
- [**Scribophile**](#) - Scribophile is an online writing and critique group for serious writers.
- [**Winvery Casino**](#) - Full featured online casino & poker accepting Bitcoins!
- [**puro express**](#) - Online Cigar shop accepting Bitcoins
- [**www.chiseeds.com**](#) - GM Free seeds, gardening advice, Moringa and more!
- [**happytreecosmetics**](#) - Natural handmade cosmetics
- [**BitMillions.com**](#) - Bet with BTC to earn Free Bitcoins Fast and Easy at the Best Provably Fair Bitcoin Lo
- [**ASAP Stuff**](#) - sells stuff in australia
- [**OZ BTC**](#) - Bitcoin classified
- [**Bits4Atmos**](#) - AtmosRX Personal Portable Vaporizers and Accessories!! AtmosRX Herb, Atmos Optimus, A
- [**Carlen Farm**](#) - Small farm producer creating maple syrup, honey and bee related products.
- [**BitArt**](#) - Web design ,Web development and programming for Bitcoins!
- [**Bitcoin Totaal**](#) - Bitcoin Shopping, Credit card, Ewallet upload, Micro Payment service and blog.
- [**buybitcoins.nl**](#) - Selling Bitcoins
- [**BitArt**](#) - Advanced web development and design solutions.
- [**Bitcoin Hypnosis Downloads**](#) - We have developed this site to provide our extensive list of self hypnosis MP3s.
- [**Paint On Screen Europe**](#) - Paint On Screen is is the leading single-coat projection screen paint.
- [**All Things Luxury**](#) - All Things Luxury offers a vast selection of jewelry and precious metals for less.
- [**mytechsolutions.com**](#) - Mytech Solutions is small personal web hosting and web development firm.
- [**VirtualOptix Networks**](#) - VirtualOptix Networks provides multiple types of internet and network solutions.
- [**SECUSRVR**](#) - SECUSRVR seeks to protect you from the Government's internet filtering.
- [**CBT Nuggets**](#) - CBT Nuggets Provides excellent Online IT training and more thorough streaming video.
- [**Age of Conquest**](#) - Age of Conquest is a medieval Risk-like turn-based strategy game.
- [**Web Kujenga Web Design and Online Marketing**](#) - Web Kujenga does online marketing and

web design for businesses of different sizes.

- [**Free Bitcoin Sites to Aid in Filling Your Wallet**](#) – A Blog that helps introduce others to the wonderful world of Bitcoin!
- [**SatoshiBet**](#) - Play Casino War for Bitcoins.
- [**Homeaway**](#) - Vacation rentals at 2.0 BTC per night
- [**Win a million**](#) - a betting site where people add Bitcoins to a shared pool.
- [**NOrCal Press**](#) - We are a PR company and record label.
- [**ledchristmaslighting.com**](#) - This website sells Holiday Lights, Halloween Costumes and other Holiday Decorations.
- [**HFBServers LLC**](#) - HFBServers is a game server provider that specializes in DayZ server hosting.
- [**Aspire Auctions, Inc.**](#) - Online Auctioneers and Appraisers of Fine Art, Antiques and Jewelry.
- [**Tripleclicks**](#) - Fast growing online marketplace and auction site. Over 71,000 products.
- [**Survival Camping Store**](#) - They sell survival gear, camping supplies, and emergency preparedness equipment.
- [**Wiser Metals**](#) - Purchase gold and silver products using BitCoin assuring privacy.
- [**More proxies**](#) - Sells proxies.
- [**Crystal Seas Kayaking Tours San Juan Islands**](#) - Premiere Active Vacations in the San Juan Islands Since 1993.
- [**BannerAdExchange.net**](#) - Our Banner Ad Exchange Program is free to join and allows any one to promote their website.
- [**Picobarn**](#) - Picobarn builds websites and provides website services.
- [**Open360.net - Virtual tours**](#) - We are in the business of making virtual tours and are accepting Bitcoins as payment.
- [**Squeaky Chairs Band**](#) - Website for local rock group rooted in Athens, Ohio. Download free music.
- [**Lunea Apartment**](#) - Lunea Apartment in Dubrovnik, Croatia, is the perfect holiday destination!
- [**The Gold Trader**](#) - The Gold Trader is a gold diamond and silver buyer and re-seller.
- [**Ontario Injury Lawyers - Canada**](#) - Car accident injury lawyers and personal injury lawyers in Ontario Canada.
- [**Pedro's Inn**](#) - Designed for the budget-minded traveler, Pedro's offers affordable Beach Access Hotel Rooms.
- [**Okotto**](#) - Okotto is a web services company providing Web Hosting, Web Design and Web Development.

Appendix C - Bitcoin Terminology

(Source: <http://www.Bitcoin.org>: With additional explanation by the author in parentheses.)

Address

A Bitcoin address is **like a physical address or an email**. It is the only information you need to provide for someone to pay you with Bitcoin. (We can have and should have for security reasons, multiple Bitcoin addresses per wallet.)

Block Chain

The block chain is a **public record of all Bitcoin transactions**, in chronological order. The block chain is shared between all Bitcoin users. It is used to verify the balance of Bitcoin addresses and to prevent **[double spending](#)**. (The block chain cleverly ties together current and future transactions with pieces of code that must “fit” together like a puzzle, verifying that they belong to the real Bitcoin network.)

Block

A block is a **record in the block chain that contains and confirms many waiting transactions**. Roughly every 10 minutes on average, a new block including transactions is appended to the **[block chain](#)** through **[mining](#)**.

BTC

BTC is the common unit of Bitcoin currency. It can be used similar to USD for US dollar instead of B_{it} or \$.

Confirmation

Confirmation means that a transaction has been **verified by the network and is highly unlikely to be reversed**. One confirmation is pretty secure. Though for larger amounts (ex. 1000 \$USD and above), one can wait for a transaction to have more confirmations - 6 is a frequently chosen number. Each new confirmation decreases the risk of a reversal exponentially. (Confirmations can take about 10 minutes when we store our wallet offline, but can be instant if they are stored online. The online wallets are part of the verification process continuously so they have instant confirmation essentially.)

Cryptography

Cryptography is the branch of mathematics that lets us create **mathematical proofs that provide high levels of security**. Online commerce and banking already uses cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the **[block chain](#)**. It can also be used to encrypt a wallet, so that it cannot be used without a password. (Bitcoin has already had an error in the code, and there are possibilities for more errors when new versions are released. This is not a perfect network, nor are there any.)

Double Spend

If a malicious user tries to **send their bitcoins to two different recipients at the same time**, this is double spending. Bitcoin **[mining](#)** and the **[block chain](#)** are there to create a consensus on the network about which of the two transactions will win.

Hash Rate

The hash rate is the **measuring unit of the processing power of the Bitcoin network**. The Bitcoin

network must make intensive mathematical operations for security purposes. When the network reaches a hash rate of 10 TH/s, it means it can make ten trillion calculations per second.

Mining

Bitcoin mining is the process of **making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions** and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Bitcoin users do Bitcoin mining and it is not an easy way to make money.

P2P

Peer to peer refers to **systems that work like an organized collective** by allowing each individual to interact directly with the others. In the case of Bitcoin, the network is built in such a way that each user is broadcasting transactions of other users. And crucially, no bank is required as a third party.

Private Key

A private key is a **secret piece of data that proves your right to spend Bitcoin from a specific Bitcoin address** through a cryptographic [signature](#). Each [Bitcoin address](#) has its own unique private key. Your private keys are stored in your computer if you use a software wallet while they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin addresses.

Signature

A [cryptographic](#) signature is a **mathematical mechanism that allows someone to prove ownership**. In the case of Bitcoin, a [Bitcoin address](#) and its [private key](#) are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the Bitcoin address. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

Wallet

A Bitcoin wallet is loosely **the equivalent of a physical wallet on the Bitcoin network**. The wallet actually contains your [private keys](#) which allow you to spend bitcoins allocated to your [Bitcoin addresses](#) in the [block chain](#). Each Bitcoin wallet can show you the total balance of all Bitcoin addresses it contains and lets you pay a specific amount to a specific person, just like a real wallet. This is different to credit cards where you are charged by the merchant.

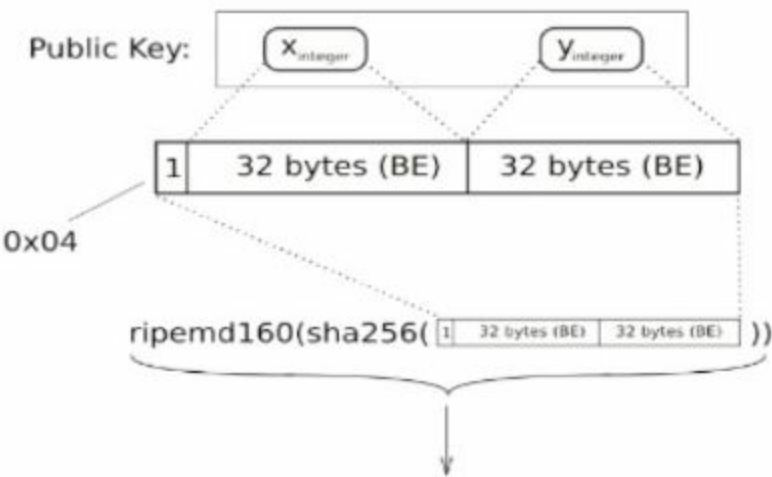
Appendix D - Bitcoins Mathematical Basis

Bitcoin Mathematical Details:

This information comes from Akram El-korashy, Computer Science and Engineering Department, German University in Cairo (<http://www.slideshare.net/akram-elkorashy/bitcoins-math>)

Bitcoin address 27-34 alphanumeric address that is a potential destination or recipient for Bitcoin payments. A Bitcoin Address is 160-digit hash of public/private portion of the ECDSA key pair. Uses a random Elliptical Curve keypair with a public key portion turned into the BTC address.

Choose a random Elliptic-Curve key-pair. The public part is converted into a BTC address



Here is what this looks like from the results of the math problems solved to create the Bitcoin Address:

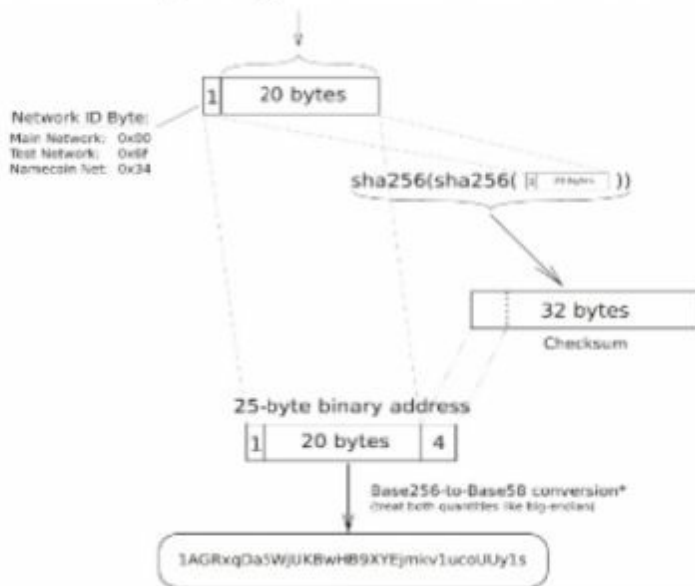
A Bitcoin Address looks like this:
1Lez1wcwPLWNmPtcfGXtSy8F34ZF45fwYh

Base58 encoding from binary to text /alphanumeric encoding except 0, O, I, l.

RIPEMD-160 is a hashing function that generates a 160 bit digest of an arbitrary block size. Essentially this function turns random words letters, numbers, etc..into a block of alphanumerics of an arbitrary number of characters of 256 bit data.

This is a critical part of the Bitcoin code that creates uniformity from the random inputs:

The 20 bytes Message Digest from RIPEMD-160..



Uses Merkle-Damgaard Construction for compressing blocks. Creating cyphers.

The basis of the math is the elliptical curve function over a field F_p is a set of points (x,y) satisfying the equation:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

There is a Signature and Verify phase of the signature algorithm.

- q is field size
- a, b are field elements
- fr is field size - and is fixed
- G is base point
- n is the order (of multiplication, how many times an element is multiplied by itself point element, group element, point doubling, etc. This is calculated from G !)
- h is a cofactor (order of the curve divided by n)

Here is what this looks like for key generation for the ECRSA form of the function as taken from the Elliptical Curve Solution Primer:

2.6.8 ECRSA

- *Key generation:*

1. B selects two distinct primes p, q with $p \equiv q \equiv 2 \bmod 3$ and computes $n = pq$;
2. B chooses integers e_B, d_B with $e_B d_B \equiv 1 \bmod (\text{lcm}(p+1, q+1))$ (he can use $(p+1)(q+1)$ in place of $\text{lcm}(p+1, q+1)$). B publishes e_B as the public key, and keeps d_B as the secret key. $\text{lcm}(a, b)$ is the lowest common multiple of a and b .

This is advanced mathematics for most readers. For a complete explanation of the math behind

elliptical curve cryptography, one of the best papers is here:
http://www.eis.mdx.ac.uk/staffpages/m_cheng/link/ecc_simple.pdf

A transaction section of data that is broadcast to the network and collected into blocks.

- It usually references previous transactions and describes sending bitcoins from one address to another. - It is not encrypted.
- Transactions and blocks are the main data structures.
- Blocks have a header and a group of transactions.
- Transactions are identified by their hash SHA-256
- Blocks are identified by a hash of the header.
- Blocks are transaction database shared by all nodes in the system using the bitcoin protocol.

Script is a set of instructions for the receiver to follow to spend the bitcoins.

Script instructions include:

- The hash of the public key should match the bitcoin address for the transaction.
- The signature of the sent date should be verifiable by the public key.
- The script includes a ECDSA signature to verify the identity of the real owner of the bitcoin address.
- Every block contains a hash of the previous block.
- Bitcoin uses the SHA-256 algorithm to generate verifiable “random” numbers that requires a predictable amount of CPU effort.

Block Chain: A block can only reference one previous block so it is impossible for two forked chains to merge.

SHA-256 is fully explained for higher-level mathematicians here:

<http://www.quadibloc.com/crypto/mi060501.htm>

GrassRootBooks.com Publishing

GrassRootBooks.com is a boutique, publishing firm that specializes in publishing fiction and non-fiction eBooks. We have a number of high-quality works currently available on the Amazon Kindle Store.

At GrassRoot Books, we work with both accomplished and up and coming authors, partnering with talent and producing high quality works. Check out our work at www.grassrootbooks.com